

Automatic License Plate Reader (ALPR)
Surveillance Use and Impact Report ANNEX

Privacy Policy (pursuant to State of California Civil Code Sections: 1798.90.51. and 798.90.53)

The State of California has Civil Code Sections which must be met for all operators of ALPR Technologies. While all the items specified herein are also detailed in the ALPR Surveillance Use and Impact Report, the Code requirements specify that they must also be detailed in a separate Privacy Policy.

California Civil Code Sections: 1798.90.51. Privacy Policy and 1798.90.53 Third Party Sharing Requirements.

An ALPR operator shall do all of the following:

(a) Maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.

The data collected by BART's ALPR system will be maintained in a secure location at BART and the Northern California Regional Intelligence Center (NCRIC), where physical access is limited to authorized individuals and includes physical access protections and firewalls.

All ALPR data used for law enforcement purposes shall be maintained in a secure manner and be encrypted via BART's IT encryption requirements from the data source capture through transmission and storage.

ALPR data will be shared with the NCRIC data center, in the NCRIC offices in the federal building in San Francisco. NCRIC facilities have 24/7 staffed security, multiple locked doors requiring both electronic keys and knowledge-based PINs. Only active NCRIC employees that also possess a valid security clearance of SECRET or better are allowed physical access.

ALPR Data used for parking efficiency and enforcement purposes will be separately stored and maintained in a secure location where physical access is limited to authorized individuals and includes physical access protections and/or firewall protections from external intrusion.

All activity is logged for audit and tracking purposes. Audits are available for an agency to view the actions of their officers.

If an ALPR operator accesses or provides access to ALPR information, the ALPR operator shall do both of the following:

(a) Maintain a record of that access. At a minimum, the record shall include all of the following:

(1) The date and time the information is accessed.

(2) The license plate number or other data elements used to query the ALPR system.

(3) The username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated.

(4) The purpose for accessing the information.

(b)(1) Implement a usage and privacy policy in order to ensure that the collection, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties. The usage and privacy policy shall be available to the public in writing, and, if the ALPR operator has an Internet Web site, the usage and privacy policy shall be posted conspicuously on that Internet Web site.

(2) The usage and privacy policy shall, at a minimum, include all of the following:

(A) The authorized purposes for using the ALPR system and collecting ALPR information.

BART ALPR Impact and Use Report specify the purpose and use and rationale why ALPR technology is used. BART's Automated License Plate Recognition (ALPR) technology seeks to increase the confidence of the public while using BART's public transportation system. Specifically, this technology seeks to improve the safety and protection of patrons, employees and their vehicles while in BART owned and operated parking areas and garages, and to improve parking enforcement. The ALPR system records vehicle license plates. Data collection shall be limited to vehicles entering or exiting and parking on BART owned and operated property. The proposed implementation of the ALPR system in BART parking areas would serve the following key purposes:

Crime Prevention

- Reduce the fear of crime and reassure the public and employees that they can safely park in BART parking facilities, which may increase BART ridership.
- Collect license plate numbers to assist in the identification, apprehension and prosecution of criminal offenders.
- Provide evidence to support the prosecution of offenders for criminal offenses.
- Provides both riders and employees a means of redress against property crimes, such as burglary and auto theft.

Efficient Parking Program Compliance

- Provides a uniform methodology for the enforcement of BART's parking rules.
- Aids in dispute mediation and provides documentation support for complaint resolution.
- Streamline parking validation.
- Help to increase ridership by determining parking lot density and space availability through and enhance efficient enforcement that parking is available only for BART passengers.
- Allow for the capability to automate parking fee collection in the future.

(B) A description of the job title or other designation of the employees and independent contractors who are authorized to use or access the ALPR system, or to collect ALPR information. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.

Access to ALPR data and images shall be restricted to the following personnel:

- All persons designated by the BART Police Department.
- Designated NCRIC Staff involved in the ALPR Administration.
- BART personnel involved in the operation, installation and maintenance of the ALPR system.
- Customer/Public Access (Restricted per the Surveillance Ordinance in item G)
- Per Court Order or Subpoena, or during an ongoing investigation.
- Office of Independent Police Auditor and Internal Affairs Department
- District Office of the General Counsel
- Authorized BART Service Providers hosting parking efficiency and enforcement applications

All personnel using BART's ALPR shall be authorized in writing and must receive training on system access and administration. ALPR system training will be provided by BART internal staff and, where necessary related, service providers. Training will consist of ALPR operation, installation, data protection and administration of the BART ALPR System and ALPR Data. Technical training will be hands on and via electronic instruction.

(C) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.

The ALPR Data Collection will be monitored by BART Police and be subject to Police and or State Auditors to ensure the security of information and compliance with applicable privacy laws.

Such data will not otherwise be disclosed/released by the BART Police Department without the consent of the Chief of Police and the Office of the General Counsel. If an ALPR operator is required to provide access to ALPR information, the ALPR operator shall do both of the following:

- (a) Maintain a record of that access. At a minimum, the record shall include the following:
 - (1) The date and time the information is accessed.
 - (2) The license plate number or other data elements used to query the ALPR system.
 - (3) The username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated.

(4) The purpose for accessing the information.

(b) Require that ALPR information only be used for the authorized purposes described in the usage and privacy policy.

(1) Indicate the authorized use; such as for criminal investigation.

As noted in the Impact and Use Reports, and the Surveillance Ordinance, the ALPR information shall only be used for the authorized purposes described therein.

(D) The purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons.

BART shall maintain robust security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. The Administrator of the data collection will not share information with Immigration and Customs Enforcement (ICE) or any agency conducting immigration enforcement or removal operations. Information is only shared with other law enforcement possessing a need and legal right to know, including the following:

- In response to subpoenas
- Pursuant to a Court Order
- Request by Law Enforcement Agencies for active Criminal Investigations
- In accordance with all applicable California State law

ALPR Data collected by BART shall not be sold under any circumstances.

(a) A public agency that operates or intends to operate an ALPR system shall provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before implementing the program.

Pursuant to the District Ordinance 2018-1, public notice and opportunity for public comment regarding the implementation of Surveillance Technology is required at Public Meetings via the BART Board of Directors Meetings; if approved then notification would be made via the BART Website and posted signs informing the public of the surveillance Technology in use.

(b) A public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only shall share data as otherwise permitted by law.

BART shall maintain robust security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. The Administrator of the data collection will not share

information with Immigration and Customs Enforcement (ICE) or any agency conducting immigration enforcement or removal operations. Information is only shared with other law enforcement possessing a need and legal right to know, including the following:

- In response to subpoenas
- Pursuant to a Court Order
- Request by Law Enforcement Agencies for active Criminal Investigations
- In accordance with all applicable California State law

ALPR Data collected by BART shall not be sold under any circumstances.

(E) The title of the official custodian, or owner, of the ALPR system responsible for implementing this section.

BART shall be the owner and official custodian of the ALPR System and any data collected there from. The BART Chief of Police, BART Office of the General Counsel and BART Police Internal Affairs will have specific oversight authority of the Program.

(F) A description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors.

ALPR system efficiency is 98% with a correct read rate of 95% resulting in proper documentation of incidents. Annual certification of the system conducted by third party calibration service parties will ensure the system is maintained at factory read rates.

(G) The length of time ALPR information will be retained, and the process the ALPR operator will utilize to determine when to destroy retained ALPR information.

Staff will adhere to the District's Surveillance Ordinance. The data from the ALPR and assorted camera system shall be collected, retained and stored in accordance with the District's Surveillance Ordinance. Data captured from the ALPR and camera system will automatically be downloaded onto a secure data storage system where it will be stored based on the systems' design and recording capabilities before being overwritten by new data; up to thirty (30) days for routine matters. Cases under active criminal investigation may be retained up to a year. Data shall not be stored beyond 1 year except by subpoena, court order or during an ongoing investigation, except in the case of data used to substantiate parking citations, which will be retained for 5 years to allow time for citation appeal and identification of scofflaws (vehicles with multiple unpaid citation). Further, the NCRIC retention policy specifies data is only retained for the period as specified by the originating agency (BART). The creation date is automatically tracked for every ALPR data point, and once the lifespan of that point is exceeded, it is removed via automated nightly processes.