

Terry Taplin  
Councilmember District 2

40

## SUPPLEMENTAL AGENDA MATERIAL for Supplemental Packet 3

**Meeting Date:** January 25, 2022

**Item Number:** 27

**Item Description:** Resolution Accepting the Surveillance Technology Report for Automatic License Plate Readers, GPS Trackers, Body Worn Cameras, and the Street Level Imagery Project Pursuant to Chapter 2.99 of the Berkeley Municipal Code

**Submitted by:** Councilmember Taplin

The District 2 office submits the following amendments to the District 4 office's supplemental for consideration:

1. Amend Section 1302.3(c)(1): replace subsection with affirmation that "existing laws prohibiting trespassing and unlawful search and seizure shall be followed."
2. Amend Section 1302.3(c)(2): append reference to existing BPD policies prohibiting harassment and intimidation, and pertinent disciplinary actions, including but not limited to General Order P-26.
3. Strike Section 1302.3(c)(6). This would prohibit the use of parking enforcement ALPR data in criminal investigations, even if parked vehicles are in a crime scene under investigation, thus endangering public safety by hindering investigatory capacity.
4. Strike Section 1302.3(c)(7). Parking Enforcement Officers (PEOs) should be able to match ALPR data to other databases where information on suspended or revoked licenses and open arrest warrants may be stored. Stolen vehicles are not the only public safety purpose in which PEOs may be of assistance.
5. Amend Section 1302.4: specify that only authorized staff may access CLETS data pursuant to the California Department of Justice's CLETS Policies, Practices, and Procedures Section 1.9.3 and Section 1.9.4.

## Surveillance Use Policy – Automatic License Plate Readers

### 1302.1 PURPOSE

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

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images for Parking Enforcement Operations and Parking Occupancy Analysis while recognizing the established privacy rights of the public.

### 1302.2 DEFINITIONS

“Alleged Parking Violation” means an alleged violation of time limits in parking areas designated by state and local law, or a violation of time limits and/or non-permit parking in the City’s RPP zones.

“ALPR Read Image” means images of license plates, vehicles, wheels or any other incidentally captured image.

“ALPR Read” means computer-readable data captured by an ALPR Reader, including ALPR Read Image and associated ALPR Read Metadata. ~~ALPR Reads are transient means to create potential government records, to include Parking Occupancy Analysis data and Enforced Citations, and therefore shall not be considered a government record itself pursuant to Government Code § 34090.6.~~

“ALPR Hit” means an Alleged Parking Violation or State Stolen ~~or Wanted~~ System alert resulting from computer generated analysis of ALPR Reads by the Genetec ALPR System resulting in an apparent:

- (1) match between an ALPR Read and ALPR Read Metadata stored in the Genetec ALPR System, to include the State Stolen ~~or Wanted~~ System; or
- (2) incongruence between an ALPR Read and permit information stored in the Passport Parking Management System.

“ALPR Read Metadata” means any image-based or other metadata, including but not limited to, global positioning system coordinates, block face information, tire position information, digitized license plates in alphanumeric characters, and timestamps.

“Automated License Plate Reader” or “ALPR” means one or more Genetec AutoVu mobile cameras affixed to Parking Enforcement Scooters and combined with computer software and algorithms to read and convert images of license plates, the characters they contain, and associated ALPR Read Metadata related to Parking Enforcement Operations or Parking Occupancy Analysis into computer-readable data.

“Deploy” or “Deployment” means any operation or use of ALPR Readers affixed to Parking Enforcement Scooters.

“Enforced ALPR Hit” means an Alleged Parking Violation confirmed by a Parking Enforcement Officer that results in the transmission of associated ALPR Read Image and ALPR Read Metadata to the Passport Parking Management System for storage in a database as a government record for the purpose of citation processing.

“Genetec ALPR System” means the computerized Genetec server and database that stores and pushes ALPR Read Metadata generated by ALPR Readers.

“Residential Parking Permits” or “RPP” means an annual, visitor, merchant or in-home care parking permit, typically represented by a vehicle’s license plate, and associated with the City’s Residential Parking Permit program across designated zones.

“Parking Enforcement Scooter” means the GO-4 three-wheeled parking enforcement vehicle.

“Parking Enforcement Officers” means employees of the City who work weekly rotations on Parking Enforcement Operations beats throughout the City and are properly trained to operate ALPRs and access the Genetec ALPR System.

“Parking Enforcement Operations” means Parking Enforcement Officer enforcement of parking regulations associated with local ordinances, the California Vehicle Code, and State Stolen ~~or Wanted~~ System enforcement through Parking Enforcement Scooter-based automated (ALPR) and non-automated means.

“Personally Identifiable Information” or “PII” means information:

- (1) that directly identifies an individual (e.g., name, address, vehicle registration number, or other identifying number or code, telephone number, email address, etc.) or
- (2) by which the City or other agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification.

“Parking Occupancy Analysis” means ongoing computational or algorithmic analyses performed by Passport Parking Management System or the City of Berkeley on ALPR Read Metadata regarding the occupancy of total parking spaces across commercial districts as part of goBerkeley, the City’s data-driven, demand-responsive parking management program. ALPR Read Metadata data associated with Parking Occupancy Analysis shall not include any license plate or other PII information.

“Parking Permit Application” means an application submitted to the City for RPP or other permit that may include but is not limited to PII such as names, address, photo identification, vehicle registration (license plate and vehicle identification number), phone number and email address.

“Passport Automatic Occupancy Data Collection System” means the server and database whereby the Passport Parking Management System vendor, on behalf of the City, downloads, stores and transfers Parking Occupancy Analysis ALPR Read

Metadata stripped of any and all PII before being transferred to the goBerkeley program.

“Passport Parking Management System” means the servers and databases maintained by Passport Labs Incorporated, containing the database of the license plate numbers and other PII associated with Parking Permit Applications and Residential Parking Permits, and including historic parking citation data, to include Enforced Hits.

“PocketPEO” means a mobile device providing handheld ticket issuance and ALPR data reference capabilities.

“State Stolen ~~or Wanted~~ System” means information from the California Law Enforcement Telecommunications System's (CLETS) Department of Motor Vehicles (DMV) Stolen Vehicle System (SVS) database providing data regarding stolen vehicles, ~~and the Federal Bureau of Investigation's National Crime Information Center (NCIC) database of and wanted vehicles.~~

### 1302.3 AUTHORIZED AND PROHIBITED USES

Use of an ALPR is restricted to the purposes outlined below.

All data and images gathered by the ALPR are for official use by the Berkeley Police Department for Parking Enforcement Operations and may be retroactively queried in limited circumstances only as specified by this policy.

~~In addition, ALPR data may be used by the Finance, Information Technology (IT), Customer Service, and Public Works Departments only as specified herein this policy, and consistent with Parking Enforcement Operations and Parking Occupancy Analysis. Since such data may contain confidential information, it is notData that is considered confidential under recent state Supreme Court rulings is not open to public review, except as specified.~~

Formatted: Not Highlight

Berkeley Police Department members or other Departments 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).

Anyone who engages in an impermissible use of the Genetec ALPR system or associated scan files or hot lists may be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

(a) An ALPR shall only be Deployed and used for Parking Enforcement Operations, and Parking Occupancy Analysis.

(b) ALPR data strictly obtained from Parking Enforcement Operations retained pursuant to this use policy, including data and metadata associated with ALPR Reads and Hits,

may be used to support a specific criminal investigation only pursuant to a valid court order, subpoena, or a search warrant.

(c) The following uses of the Genetec ALPR System are specifically prohibited:

(1) Invasion of Privacy

~~Except when done pursuant to a court order, subpoena, or a search warrant, it 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). Existing laws prohibiting trespassing and unlawful search and seizure shall be followed.~~

(2) Harassment or Intimidation

It is a violation of this Policy to use the Genetec ALPR system to harass and/or intimidate any individual or group, pursuant to BPD General Order P-26.

(3) Use Based on a Protected Characteristic.

It is a violation of this Policy to use the ALPRs 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 state and federal law.

(4) Personal Use

It is a violation of this Policy to use the Genetec ALPR System or associated ALPR Read data or the State Stolen or Wanted System hot lists for any personal purpose.

(5) First Amendment Rights

It is a violation of this Policy to use ALPRs or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

~~(6) Criminal Enforcement~~

~~It is a violation of this Policy to use or Deploy ALPRs to scan or canvass license plates in connection with any crime scene, patrol operation, or investigation.~~

~~(7) Use of Hot Lists~~

~~It is a violation of this Policy to use the Genetec ALPR System in conjunction with any hot list other than the State Stolen or Wanted System.~~

**1302.4 DATA COLLECTION AND RETENTION**

The Investigations Division Captain, or their designee, is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by the City of Berkeley's IT department and associated Genetec ALPR system providers/vendors as identified below.

IT's role will be limited to providing initial infrastructure set-up and accessing or viewing individual records or reports (potentially including PII or CLETS information as authorized by the Chief of Police), limited to the purposes of testing the accuracy of the equipment. Genetec ALPR System data provided to Parking Control Officers may also contain confidential CLETS information and is not open to public review.

ALPR information gathered and retained by the Berkeley Police Department may only be used and shared with prosecutors or other law enforcement agencies pursuant to a valid court order, subpoena, or a search warrant and as limited by this policy.

(a) ALPR Read Images

ALPR Read Images ~~and Metadata~~ resulting from ALPR Reads stored locally on Parking Control Officer Vehicle laptops and PocketPEO shall be purged at least nightly.

In no case shall ALPR Read Images resulting from ALPR Reads be transmitted to or stored in the Genetec ALPR System.

(b) ALPR Reads Not Resulting in ALPR Hits

All ALPR Read Metadata from ALPR Reads transmitted and stored in the Genetec ALPR System shall be purged within five (5) days consistent with the City's 72-Hour Rule (BMC Section 14.36.050).

In no case shall ALPR Read Metadata in the form of license plate data or other PII be transmitted to or stored in the Passport Automatic Occupancy Data Collection System.

(c) ALPR Hits

All ALPR ~~Read Images, Metadata, and Hits~~ resulting from ALPR Reads stored locally on Parking Control Officer Vehicle laptops and PocketPEO shall be purged at least nightly.

In no case shall data associated with ALPR Hits be transmitted to or stored in the Genetec ALPR System, nor shall license plate data or other PII included as part of ALPR Read Metadata be transmitted to or stored by the City for Parking Occupancy Analysis (goBerkeley), to include the Passport Automatic Occupancy Data Collection System or as City Department records.

(d) Unenforced ALPR Hits

All erroneous and unenforced ALPR Hit data and Read Metadata shall be purged locally at least nightly.

(e) Enforced ALPR Hits

Only ALPR Read Images and Metadata associated with Enforced ALPR Hits shall be downloaded to the Passport Parking Management servers with a minimum retention period 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 action pursuant to a valid court order, subpoena, or a search warrant or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

### 1302.5 DATA ACCESS

(a) Only properly trained Parking Control Officers and information technology personnel are allowed access to the Genetec ALPR system or to collect ALPR information.

(b) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training, which shall include complying with this use policy.

(c) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so pursuant to California Department of Justice's CLETS Policies, Practices, and Procedures Section 1.9.3 and Section 1.9.4

~~(c)~~ If a Sworn officer is called to verify a stolen vehicle, 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 Hit.

~~(e) Police will not take any police action that restricts the freedom of any individual based solely on an ALPR Hit unless it has been validated as described above in (d).~~

~~(1) Police 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.~~

~~(2) Prior to initiation of a stop of a vehicle or other intervention based on an ALPR Hit, Department members shall undertake the following:~~

~~(i) Verification of status on State Stolen or Wanted System.~~

~~An officer must receive confirmation from a Police Department Communications Dispatcher or other department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).~~

~~(ii) Visual verification of license plate number.~~

(d) Sworn Officers shall visually verify that the license plate of interest matches identically with the ALPR Read Image of the license plate number captured (ALPR Read) by the ALPR, 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 an ALPR Hit in a specific State Stolen ~~or Wanted~~-System 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.

#### **1302.6 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. 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 impacts that may violate the First and Fourth Amendments and other potentially disparate or adverse impacts on any communities or groups.

The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for the purpose of 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 (CPB).

#### **1302.7 PUBLIC ACCESS**

Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requester in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

#### **1302.8 THIRD-PARTY DATA-SHARING**

(a) Non-law enforcement requests for access to stored ALPR data related to parking management shall be processed according to this policy, and the Records Maintenance and Release Policy in accordance with applicable law.

(b) The ALPR data may be shared only with other law enforcement or prosecutorial agencies ~~for official law enforcement purposes or~~ as permitted by this policy ~~and under~~

Formatted: Strikethrough



~~no circumstances- ALPR data is subject to the provisions of BPD Policy 415, and hence may not~~ be shared with federal immigration enforcement officials.

Formatted: Strikethrough

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided by this policy and in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

Aggregated ALPR data not related to specific criminal investigations authorized by a court order, subpoena, or search warrant shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager and only in accordance with this Use Policy.

Third-party data-sharing shall be subject to non-privileged and non-confidential City Council notification pursuant to BMC 2.99.020 (2) (a).

### **1302.9 TRAINING AND ALPR ADMINISTRATOR**

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.

(1) The Investigations Division Captain shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(i) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the Genetec ALPR system or to collect ALPR information.

(ii) Ensuring that training requirements are completed for authorized users. The Administrator shall ensure that members receive department-approved training for those authorized to use or access ALPRs (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

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

(iv) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52 and this Use Policy.

(v) The title and name of the current designee in overseeing the ALPR operation.

(vi) Ensuring this policy and related procedures are conspicuously posted on the City's website.

### **1302.10 AUDITING AND OVERSIGHT**

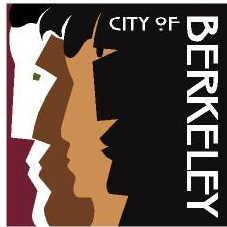
Genetec ALPR System audits will be conducted by the Professional Standards Bureau's (PSD) Audit and Inspections Sergeant pursuant to ~~Municipal Code Section~~BMC 2.99.020 4. k. on a regular basis, at least biannually.

(1) Any unauthorized access or data breach shall be reported immediately to the City Manager.

(2) 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 by PSD.

#### **1302.11 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 their command to administer the day-to-day operation of the ALPR equipment and data.



Kate Harrison  
Councilmember District 4

## REVISED AGENDA MATERIAL for Supplemental Packet 2

**Meeting Date:** November 30, 2021

**Item Number:** 27

**Item Description:** Resolution Accepting the Surveillance Technology Report for Automatic License Plate Readers, GPS Trackers, Body Worn Cameras, and the Street Level Imagery Project Pursuant to Chapter 2.99 of the Berkeley Municipal Code

**Submitted by:** Councilmember Harrison

The supplemental includes updates to the ALPR Use Policy as follows:

- Removes reference to Government Code Section 34090 consistent with SB 34 (providing for a local government to set ALPR retention limits).
- Clarifies that the definition of the State Stolen System includes the DMV's SVS database.
- Clarifies the type of data that is considered confidential pursuant to recent State Supreme Court rulings.
- Fixes inconsistency under the "Invasion of Privacy" section.
- Adds missing reference to state and federal law under "Use Based on a Protected Characteristic" section.
- Clarifies IT's role in maintaining accuracy and functionality of ALPR equipment.
- Further clarifies distinction between ALPR Read Images and ALPR Hits.
- Strikes extraneous language regarding Sworn Officer stolen vehicle verification procedures.
- Clarifies that ALPR data may only be shared with law enforcement or prosecutorial agencies as permitted by the Policy.
- Adds specific references to BMC sections under the auditing and oversight section.
- Adds other non-substantive changes.

## Surveillance Use Policy – Automatic License Plate Readers

### 1302.1 PURPOSE

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

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images for Parking Enforcement Operations and Parking Occupancy Analysis while recognizing the established privacy rights of the public.

### 1302.2 DEFINITIONS

“Alleged Parking Violation” means an alleged violation of time limits in parking areas designated by state and local law, or a violation of time limits and/or non-permit parking in the City’s RPP zones.

“ALPR Read Image” means images of license plates, vehicles, wheels or any other incidentally captured image.

“ALPR Read” means computer-readable data captured by an ALPR Reader, including ALPR Read Image and associated ALPR Read Metadata. ALPR Reads are transient means to create potential government records, to include Parking Occupancy Analysis data and Enforced Citations, ~~and therefore shall not be considered a government record itself pursuant to Government Code § 34090.6.~~

“ALPR Hit” means an Alleged Parking Violation or State Stolen ~~or Wanted~~ System alert resulting from computer generated analysis of ALPR Reads by the Genetec ALPR System resulting in an apparent:

- (1) match between an ALPR Read and ALPR Read Metadata stored in the Genetec ALPR System, to include the State Stolen ~~or Wanted~~ System; or
- (2) incongruence between an ALPR Read and permit information stored in the Passport Parking Management System.

“ALPR Read Metadata” means any image-based or other metadata, including but not limited to, global positioning system coordinates, block face information, tire position information, digitized license plates in alphanumeric characters, and timestamps.

“Automated License Plate Reader” or “ALPR” means one or more Genetec AutoVu mobile cameras affixed to Parking Enforcement Scooters and combined with computer software and algorithms to read and convert images of license plates, the characters they contain, and associated ALPR Read Metadata related to Parking Enforcement Operations or Parking Occupancy Analysis into computer-readable data.

“Deploy” or “Deployment” means any operation or use of ALPR Readers affixed to Parking Enforcement Scooters.

“Enforced ALPR Hit” means an Alleged Parking Violation confirmed by a Parking Enforcement Officer that results in the transmission of associated ALPR Read Image and ALPR Read Metadata to the Passport Parking Management System for storage in a database as a government record for the purpose of citation processing.

“Genetec ALPR System” means the computerized Genetec server and database that stores and pushes ALPR Read Metadata generated by ALPR Readers.

“Residential Parking Permits” or “RPP” means an annual, visitor, merchant or in-home care parking permit, typically represented by a vehicle’s license plate, and associated with the City’s Residential Parking Permit program across designated zones.

“Parking Enforcement Scooter” means the GO-4 three-wheeled parking enforcement vehicle.

“Parking Enforcement Officers” means employees of the City who work weekly rotations on Parking Enforcement Operations beats throughout the City and are properly trained to operate ALPRs and access the Genetec ALPR System.

“Parking Enforcement Operations” means Parking Enforcement Officer enforcement of parking regulations associated with local ordinances, the California Vehicle Code, and State Stolen ~~or Wanted~~ System enforcement through Parking Enforcement Scooter-based automated (ALPR) and non-automated means.

“Personally Identifiable Information” or “PII” means information:

- (1) that directly identifies an individual (e.g., name, address, vehicle registration number, or other identifying number or code, telephone number, email address, etc.) or
- (2) by which the City or other agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification.

“Parking Occupancy Analysis” means ongoing computational or algorithmic analyses performed by Passport Parking Management System or the City of Berkeley on ALPR Read Metadata regarding the occupancy of total parking spaces across commercial districts as part of goBerkeley, the City’s data-driven, demand-responsive parking management program. ALPR Read Metadata data associated with Parking Occupancy Analysis shall not include any license plate or other PII information.

“Parking Permit Application” means an application submitted to the City for RPP or other permit that may include but is not limited to PII such as names, address, photo identification, vehicle registration (license plate and vehicle identification number), phone number and email address.

“Passport Automatic Occupancy Data Collection System” means the server and database whereby the Passport Parking Management System vendor, on behalf of the City, downloads, stores and transfers Parking Occupancy Analysis ALPR Read

Metadata stripped of any and all PII before being transferred to the goBerkeley program.

“Passport Parking Management System” means the servers and databases maintained by Passport Labs Incorporated, containing the database of the license plate numbers and other PII associated with Parking Permit Applications and Residential Parking Permits, and including historic parking citation data, to include Enforced Hits.

“PocketPEO” means a mobile device providing handheld ticket issuance and ALPR data reference capabilities.

“State Stolen ~~or Wanted~~ System” means information from the California Law Enforcement Telecommunications System's (CLETS) Department of Motor Vehicles (DMV) Stolen Vehicle System (SVS) database providing data regarding stolen vehicles, ~~and the Federal Bureau of Investigation's National Crime Information Center (NCIC) database of and wanted vehicles.~~

### 1302.3 AUTHORIZED AND PROHIBITED USES

Use of an ALPR is restricted to the purposes outlined below.

All data and images gathered by the ALPR are for official use by the Berkeley Police Department for Parking Enforcement Operations and may be retroactively queried in limited circumstances only as specified by this policy.

In addition, ALPR data may be used by the Finance, Information Technology (IT), Customer Service, and Public Works Departments only as specified ~~herein~~ this policy, and consistent with Parking Enforcement Operations and Parking Occupancy Analysis. ~~Since such data may contain confidential information, it is not~~ Data that is considered confidential under recent state Supreme Court rulings is not open to public review, ~~except as specified.~~

Berkeley Police Department members or other Departments 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).

Anyone who engages in an impermissible use of the Genetec ALPR system or associated scan files or hot lists may be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

(a) An ALPR shall only be Deployed and used for Parking Enforcement Operations, and Parking Occupancy Analysis.

(b) ALPR data strictly obtained from Parking Enforcement Operations retained pursuant to this use policy, including data and metadata associated with ALPR Reads and Hits, may be used to support a specific criminal investigation only pursuant to a valid court order, subpoena, or a search warrant.

(c) The following uses of the Genetec ALPR System are specifically prohibited:

(1) Invasion of Privacy

~~Except when done pursuant to a court order, subpoena, or a search warrant, i~~ it 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 Genetec 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 ALPRs 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 state and federal law.

(4) Personal Use

It is a violation of this Policy to use the Genetec ALPR System or associated ALPR Read data or the State Stolen ~~or Wanted~~-System hot lists for any personal purpose.

(5) First Amendment Rights

It is a violation of this Policy to use ALPRs or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

(6) Criminal Enforcement

It is a violation of this Policy to use or Deploy ALPRs to scan or canvass license plates in connection with any crime scene, patrol operation, or investigation.

(7) Use of Hot Lists

It is a violation of this Policy to use the Genetec ALPR System in conjunction with any hot list other than the State Stolen ~~or Wanted~~-System.

### 1302.4 DATA COLLECTION AND RETENTION

The Investigations Division Captain, or their designee, is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by the City of Berkeley's IT department and associated Genetec ALPR system providers/vendors as identified below.

IT's role will be limited to providing initial infrastructure set-up and accessing or viewing individual records or reports (potentially including PII or CLETS information as authorized by the Chief of Police), limited to the purposes of testing the accuracy of the equipment. Genetec ALPR System data provided to Parking Control Officers may also contain confidential CLETS information and is not open to public review.

ALPR information gathered and retained by the Berkeley Police Department may only be used and shared with prosecutors or other law enforcement agencies pursuant to a valid court order, subpoena, or a search warrant and as limited by this policy.

(a) ALPR Read Images

ALPR Read Images and Metadata resulting from ALPR Reads stored locally on Parking Control Officer Vehicle laptops and PocketPEO shall be purged at least nightly.

In no case shall ALPR Read Images resulting from ALPR Reads be transmitted to or stored in the Genetec ALPR System.

(b) ALPR Reads Not Resulting in ALPR Hits

All ALPR Read Metadata from ALPR Reads transmitted and stored in the Genetec ALPR System shall be purged within five (5) days consistent with the City's 72-Hour Rule (BMC Section 14.36.050).

In no case shall ALPR Read Metadata in the form of license plate data or other PII be transmitted to or stored in the Passport Automatic Occupancy Data Collection System.

(c) ALPR Hits

All ALPR Read Images, Metadata, and Hits resulting from ALPR Reads stored locally on Parking Control Officer Vehicle laptops and PocketPEO shall be purged at least nightly.

In no case shall data associated with ALPR Hits be transmitted to or stored in the Genetec ALPR System, nor shall license plate data or other PII included as part of ALPR Read Metadata be transmitted to or stored by the City for Parking Occupancy Analysis (goBerkeley), to include the Passport Automatic Occupancy Data Collection System or as City Department records.

(d) Unenforced ALPR Hits

All erroneous and unenforced ALPR Hit data and Read Metadata shall be purged locally at least nightly.

(e) Enforced ALPR Hits

Only ALPR Read Images and Metadata associated with Enforced ALPR Hits shall be downloaded to the Passport Parking Management servers with a minimum retention period 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 action pursuant to a valid court order, subpoena, or a search warrant or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

### 1302.5 DATA ACCESS

(a) Only properly trained Parking Control Officers and information technology personnel are allowed access to the Genetec ALPR system or to collect ALPR information.

(b) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training, which shall include complying with this use policy.

(c) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.

~~(cd)~~ If a Sworn officer is called to verify a stolen vehicle, 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 Hit.

~~(e) Police will not take any police action that restricts the freedom of any individual based solely on an ALPR Hit unless it has been validated as described above in (d).~~

~~(1) Police 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.~~

~~(2) Prior to initiation of a stop of a vehicle or other intervention based on an ALPR Hit, Department members shall undertake the following:~~

~~(i) Verification of status on State Stolen or Wanted System.~~

~~An officer must receive confirmation from a Police Department Communications Dispatcher or other department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).~~

~~(ii) Visual verification of license plate number.~~

(d) Sworn Officers shall visually verify that the license plate of interest matches identically with the ALPR Read Image of the license plate number captured (ALPR Read) by the ALPR, 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 an ALPR Hit in a specific State Stolen ~~or Wanted~~ System 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.

### **1302.6 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. 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 impacts that may violate the First and Fourth Amendments and other potentially disparate or adverse impacts on any communities or groups.

The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for the purpose of 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 (CPB).

### **1302.7 PUBLIC ACCESS**

Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requester in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

### **1302.8 THIRD-PARTY DATA-SHARING**

(a) Non-law enforcement requests for access to stored ALPR data related to parking management shall be processed according to this policy, and the Records Maintenance and Release Policy in accordance with applicable law.

(b) The ALPR data may be shared only with other law enforcement or prosecutorial agencies ~~for official law enforcement purposes or~~ as permitted by this policy and under no circumstances: ALPR data is subject to the provisions of BPD Policy 415, and hence may not be shared with federal immigration enforcement officials.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided by this policy and in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

Aggregated ALPR data not related to specific criminal investigations authorized by a court order, subpoena, or search warrant shall not be released to any local, state or

federal agency or entity without the express written consent of the City Manager and only in accordance with this Use Policy.

Third-party data-sharing shall be subject to non-privileged and non-confidential City Council notification pursuant to BMC 2.99.020 (2) (a).

### **1302.9 TRAINING AND ALPR ADMINISTRATOR**

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.

(1) The Investigations Division Captain shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(i) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the Genetec ALPR system or to collect ALPR information.

(ii) Ensuring that training requirements are completed for authorized users. The Administrator shall ensure that members receive department-approved training for those authorized to use or access ALPRs (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

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

(iv) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52 and this Use Policy.

(v) The title and name of the current designee in overseeing the ALPR operation.

(vi) Ensuring this policy and related procedures are conspicuously posted on the City's website.

### **1302.10 AUDITING AND OVERSIGHT**

Genetec ALPR System audits will be conducted by the Professional Standards Bureau's (PSD) Audit and Inspections Sergeant pursuant to Municipal Code Section BMC 2.99.020 4. k. on a regular basis, at least biannually.

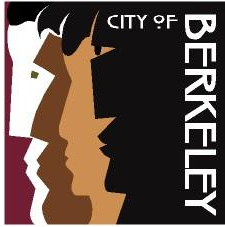
(1) Any unauthorized access or data breach shall be reported immediately to the City Manager.

(2) 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 by PSD.

### **1302.11 MAINTENANCE**

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under their command to administer the day-to-day operation of the ALPR equipment and data.



Kate Harrison  
Councilmember District 4

## REVISED AGENDA MATERIAL for Supplemental Packet 1

**Meeting Date:** November 30, 2021

**Item Number:** 27

**Item Description:** Resolution Accepting the Surveillance Technology Report for Automatic License Plate Readers, GPS Trackers, Body Worn Cameras, and the Street Level Imagery Project Pursuant to Chapter 2.99 of the Berkeley Municipal Code

**Submitted by:** Councilmembers Harrison and Hahn

Amends Resolution to adopt a Surveillance Technology Use Policy for Automatic License Plate Readers as required by the Surveillance Technology Ordinance.

To date, Council deferred adoption of a Surveillance Use Policy pursuant to Sections 2.99.020 and 2.99.050 of the Ordinance for Automatic License Plate Readers, including in order to draft a policy with enhanced civil liberties protections. Berkeley Police Department Administrative Order #001-2016, prepared in 2016 before adoption of the Surveillance Ordinance, has served as a de facto ALPR policy, however Administrative Order #001-2016 is out of date and does not satisfy the specific requirements of the Surveillance Ordinance. Adoption of an earlier proposed update to the use policy for ALPRs was deferred by Council as it did not contain sufficient information about data retention and sharing and protection of civil liberties.

The attached Use Policy supersedes Administrative Order #001-2016 and satisfies the requirements of the Ordinance, including providing a legally-enforceable Surveillance Use Policy and enhanced civil liberties protections.

### Use Policy Overview:

- Provides key definitions.
- Authorizes ALPR for Parking Enforcement Operations and Parking Occupancy Analysis.
- Enumerates specifically prohibited uses of ALPR that may impact civil liberties.
- Incorporates key provisions from BPD's previously proposed Policy 1302.

- Addresses the Police Review Commission's concerns, as expressed in their September 11, 2019 letter to Council pursuant to Section 2.99.030, about the previously proposed Use Policy 1302.
- Specifies appropriate data retention periods for ALPR reads and hits.
- Specifies that personally identifiable ALPR data will not be sent to goBerkeley (as confirmed by Transportation Division staff) as part of Parking Occupancy Analysis.
- Specifies that ALPR data obtained from Parking Enforcement Operations, including data and metadata associated with ALPR Reads and Hits, may be used to support a specific criminal investigation only pursuant to a valid court order, subpoena, or a search warrant.
- Restates the City's policy of not sharing of ALPR data gathered by the City or its contractors/subcontractors for purpose of federal immigration enforcement.
- Specifies that third-party data-sharing shall be subject to non-privileged and non-confidential City Council notification pursuant to BMC 2.99.020.

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

A RESOLUTION ACCEPTING THE ANNUAL SURVEILLANCE TECHNOLOGY REPORT FOR AUTOMATIC LICENSE PLATE READERS, GPS TRACKERS, BODY WORN CAMERAS, AND THE STREET LEVEL IMAGERY PROJECT AND ADOPTING A SURVEILLANCE TECHNOLOGY USE POLICY FOR AUTOMATIC LICENSE PLATE READERS

WHEREAS, on March 27, 2018, the City Council adopted Ordinance 7,592-N.S., which is known as the Surveillance Technology Use and Community Safety Ordinance (“Ordinance”); and

WHEREAS, Section 2.99.070 of the Ordinance requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance at the first regular City Council meeting in November; and

WHEREAS, the Surveillance Technology Reports satisfy the requirements of the Ordinance-; and

WHEREAS, Council deferred adoption of a Surveillance Use Policy pursuant to Sections 2.99.020 and 2.99.050 of the Ordinance for Automatic License Plate Readers in order to draft a policy with enhanced civil liberties protections, and heretofore Berkeley Police Department Administrative Order #001-2016, prepared in 2016 before passage of the Surveillance Ordinance, has served as a de facto ALPR policy; and

WHEREAS, the attached Use Policy supersedes Administrative Order #001-2016 and satisfies the requirements of the Ordinance, including providing a legally-enforceable Surveillance Use Policy and enhanced civil liberties protections.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the Council hereby accepts the Surveillance Technology Reports for Automatic License Plate Readers, GPS Trackers, Body Worn Cameras, and the Street Level Imagery Project and adopts a Surveillance Technology Use Policy for Automatic License Plate Readers.

Attachment

1. Surveillance Use Policy – Automatic License Plate Readers

## Surveillance Use Policy – Automatic License Plate Readers

### 1302.1 PURPOSE

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

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images for Parking Enforcement Operations and Parking Occupancy Analysis while recognizing the established privacy rights of the public.

### 1302.2 DEFINITIONS

“Alleged Parking Violation” means an alleged violation of time limits in parking areas designated by state and local law, or a violation of time limits and/or non-permit parking in the City’s RPP zones.

“ALPR Read Image” means images of license plates, vehicles, wheels or any other incidentally captured image.

“ALPR Read” means computer-readable data captured by an ALPR Reader, including ALPR Read Image and associated ALPR Read Metadata. ALPR Reads are transient means to create potential government records, to include Parking Occupancy Analysis data and Enforced Citations, and therefore shall not be considered a government record itself pursuant to Government Code § 34090.6.

“ALPR Hit” means an Alleged Parking Violation or State Stolen or Wanted System alert resulting from computer generated analysis of ALPR Reads by the Genetec ALPR System resulting in an apparent:

- (1) match between an ALPR Read and ALPR Read Metadata stored in the Genetec ALPR System, to include the State Stolen or Wanted System; or
- (2) incongruence between an ALPR Read and permit information stored in the Passport Parking Management System.

“ALPR Read Metadata” means any image-based or other metadata, including but not limited to, global positioning system coordinates, block face information, tire position information, digitized license plates in alphanumeric characters, and timestamps.

“Automated License Plate Reader” or “ALPR” means one or more Genetec AutoVu mobile cameras affixed to Parking Enforcement Scooters and combined with computer software and algorithms to read and convert images of license plates, the characters they contain, and associated ALPR Read Metadata related to Parking Enforcement Operations or Parking Occupancy Analysis into computer-readable data.

“Deploy” or “Deployment” means any operation or use of ALPR Readers affixed to Parking Enforcement Scooters.



“Enforced ALPR Hit” means an Alleged Parking Violation confirmed by a Parking Enforcement Officer that results in the transmission of associated ALPR Read Image and ALPR Read Metadata to the Passport Parking Management System for storage in a database as a government record for the purpose of citation processing.

“Genetec ALPR System” means the computerized Genetec server and database that stores and pushes ALPR Read Metadata generated by ALPR Readers.

“Residential Parking Permits” or “RPP” means an annual, visitor, merchant or in-home care parking permit, typically represented by a vehicle’s license plate, and associated with the City’s Residential Parking Permit program across designated zones.

“Parking Enforcement Scooter” means the GO-4 three-wheeled parking enforcement vehicle.

“Parking Enforcement Officers” means employees of the City who work weekly rotations on Parking Enforcement Operations beats throughout the City and are properly trained to operate ALPRs and access the Genetec ALPR System.

“Parking Enforcement Operations” means Parking Enforcement Officer enforcement of parking regulations associated with local ordinances, the California Vehicle Code, and State Stolen or Wanted System enforcement through Parking Enforcement Scooter-based automated (ALPR) and non-automated means.

“Personally Identifiable Information” or “PII” means information:

- (1) that directly identifies an individual (e.g., name, address, vehicle registration number, or other identifying number or code, telephone number, email address, etc.) or
- (2) by which the City or other agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification.

“Parking Occupancy Analysis” means ongoing computational or algorithmic analyses performed by Passport Parking Management System or the City of Berkeley on ALPR Read Metadata regarding the occupancy of total parking spaces across commercial districts as part of goBerkeley, the City’s data-driven, demand-responsive parking management program. ALPR Read Metadata data associated with Parking Occupancy Analysis shall not include any license plate or other PII information.

“Parking Permit Application” means an application submitted to the City for RPP or other permit that may include but is not limited to PII such as names, address, photo identification, vehicle registration (license plate and vehicle identification number), phone number and email address.

“Passport Automatic Occupancy Data Collection System” means the server and database whereby the Passport Parking Management System vendor, on behalf of the City, downloads, stores and transfers Parking Occupancy Analysis ALPR Read

Metadata stripped of any and all PII before being transferred to the goBerkeley program.

“Passport Parking Management System” means the servers and databases maintained by Passport Labs Incorporated, containing the database of the license plate numbers and other PII associated with Parking Permit Applications and Residential Parking Permits, and including historic parking citation data, to include Enforced Hits.

“PocketPEO” means a mobile device providing handheld ticket issuance and ALPR data reference capabilities.

“State Stolen or Wanted System” means information from the California Law Enforcement Telecommunications System's (CLETS) Department of Motor Vehicles (DMV) Stolen Vehicle System (SVS) database providing data regarding stolen vehicles, and the Federal Bureau of Investigation's National Crime Information Center (NCIC) database of wanted vehicles.

### **1302.3 AUTHORIZED AND PROHIBITED USES**

Use of an ALPR is restricted to the purposes outlined below.

All data and images gathered by the ALPR are for official use by the Berkeley Police Department for Parking Enforcement Operations and may be retroactively queried in limited circumstances only as specified by this policy.

In addition, ALPR data may be used by the Finance, Information Technology (IT), Customer Service, and Public Works Departments as specified herein and consistent with Parking Enforcement Operations and Parking Occupancy Analysis. Since such data may contain confidential information, it is not open to public review, except as specified.

Berkeley Police Department members or other Departments 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).

Anyone who engages in an impermissible use of the Genetec ALPR system or associated scan files or hot lists may be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

(a) An ALPR shall only be Deployed and used for Parking Enforcement Operations, and Parking Occupancy Analysis.

(b) ALPR data strictly obtained from Parking Enforcement Operations, including data and metadata associated with ALPR Reads and Hits, may be used to support a specific criminal investigation only pursuant to a valid court order, subpoena, or a search warrant.

(c) The following uses of the Genetec ALPR System are specifically prohibited:

(1) Invasion of Privacy

Except when done pursuant to a court order, subpoena, or a search warrant, it 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 Genetec 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 ALPRs 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

(4) Personal Use

It is a violation of this Policy to use the Genetec ALPR System or associated ALPR Read data or State Stolen or Wanted System lists for any personal purpose.

(5) First Amendment Rights

It is a violation of this Policy to use ALPRs or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

(6) Criminal Enforcement

It is a violation of this Policy to use or Deploy ALPRs to scan or canvass license plates in connection with any crime scene, patrol operation, or investigation.

(7) Use of Hot Lists

It is a violation of this Policy to use the Genetec ALPR System in conjunction with any hot list other than the State Stolen or Wanted System.

**1302.4 DATA COLLECTION AND RETENTION**

The Investigations Division Captain, or their designee, is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by the City of Berkeley's IT department and associated Genetec ALPR system providers/vendors as identified below.

IT staff will not have the ability to access or view individual records or reports, as they may contain PII information they are not authorized to receive. Genetec ALPR System

data provided to Parking Control Officers may also contain confidential CLETS information and is not open to public review. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive PII or CLETS information.

ALPR information gathered and retained by the Berkeley Police Department may only be used and shared with prosecutors or other law enforcement agencies pursuant to a valid court order, subpoena, or a search warrant and as limited by this policy.

(a) ALPR Reads

ALPR Read Images and Metadata resulting from ALPR Reads stored locally on Parking Control Officer Vehicle laptops and PocketPEO shall be purged at least nightly.

In no case shall ALPR Read Images resulting from ALPR Reads be transmitted to or stored in the Genetec ALPR System.

(b) ALPR Reads Not Resulting in ALPR Hits

All ALPR Read Metadata from ALPR Reads transmitted and stored in the Genetec ALPR System shall be purged within five (5) days consistent with the City's 72-Hour Rule (BMC Section 14.36.050).

In no case shall ALPR Read Metadata in the form of license plate data or other PII be transmitted to or stored in the Passport Automatic Occupancy Data Collection System.

(c) ALPR Hits

All ALPR Read Images, Metadata, and Hits resulting from ALPR Reads stored locally on Parking Control Officer Vehicle laptops and PocketPEO shall be purged at least nightly.

In no case shall data associated with ALPR Hits be transmitted to or stored in the Genetec ALPR System, or license plate data or other PII included as part of ALPR Read Metadata be transmitted to or stored by the City for Parking Occupancy Analysis, to include the Passport Automatic Occupancy Data Collection System or as City Department records.

(d) Unenforced ALPR Hits

All erroneous and unenforced ALPR Hit data and Read Metadata shall be purged locally at least nightly.

(e) Enforced ALPR Hits

Only ALPR Read Images and Metadata associated with Enforced ALPR Hits shall be downloaded to the Passport Parking Management servers with a minimum retention period 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 action pursuant to a valid court order, subpoena, or a search warrant or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

### **1302.5 DATA ACCESS**

- (a) Only properly trained parking control officers and information technology personnel are allowed access to the Genetec ALPR system or to collect ALPR information.
- (b) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- (c) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.
- (d) 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 Hit.
- (e) Police will not take any police action that restricts the freedom of any individual based solely on an ALPR Hit unless it has been validated.
  - (1) Police 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.
  - (2) Prior to initiation of a stop of a vehicle or other intervention based on an ALPR Hit, Department members shall undertake the following:
    - (i) Verification of status on State Stolen or Wanted System.

An officer must receive confirmation from a Police Department Communications Dispatcher or other department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).

- (ii) Visual verification of license plate number.

Officers shall visually verify that the license plate of interest matches identically with the ALPR Read Image of the license plate number captured (ALPR Read) by the ALPR, 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 an ALPR Hit in a specific State Stolen or Wanted System 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.

### **1302.6 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. 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 impacts that may violate the First and Fourth Amendments and other potentially disparate or adverse impacts on any communities or groups.

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, 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 (CPB).

### **1302.7 PUBLIC ACCESS**

(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) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requester in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

### **1302.8 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 permitted by this policy. ALPR data is subject to the provisions of BPD Policy 415, and hence may not be shared with federal immigration enforcement officials.

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).

Aggregated ALPR data not related to specific criminal investigations authorized by a court order, subpoena, or search warrant shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.

Third-party data-sharing shall be subject to non-privileged and non-confidential City Council notification pursuant to BMC 2.99.020 (2) (a).

### **1302.9 TRAINING AND ALPR ADMINISTRATOR**

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.

(1) The Investigations Division Captain shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(i) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the Genetec ALPR system or to collect ALPR information.

(ii) Ensuring that training requirements are completed for authorized users. The Administrator shall ensure that members receive department-approved training for those authorized to use or access ALPRs (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

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

(iv) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.

(v) The title and name of the current designee in overseeing the ALPR operation.

(vi) Ensuring this policy and related procedures are conspicuously posted on the City's website.

### **1302.10 AUDITING AND OVERSIGHT**

Genetec ALPR System audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant pursuant to Municipal Code Section 2.99 on a regular basis, at least biannually.

(1) Any unauthorized access or data breach shall be reported immediately to the City Manager.

(2) 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 Section 2.99, published on the City of Berkeley website in an appropriate location, and retained by PSD.

### **1302.11 MAINTENANCE**

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under their command to administer the day-to-day operation of the ALPR equipment and data.





Office of the City Manager

ACTION CALENDAR

March 22, 2022

*(Continued from January 25, 2022)*

To: Honorable Mayor and Members of the City Council

From: Dee Williams-Ridley, City Manager

Submitted by: Jennifer Louis, Interim Chief of Police  
LaTanya Bellow, Interim Deputy City Manager

Subject: Resolution Accepting the Surveillance Technology Report for Automatic License Plate Readers, GPS Trackers, Body Worn Cameras, and the Street Level Imagery Project Pursuant to Chapter 2.99 of the Berkeley Municipal Code

RECOMMENDATION

Adopt a Resolution accepting the Surveillance Technology Report for Automatic License Plate Readers, GPS Trackers, Body Worn Cameras, and the Street Level Imagery Project Pursuant to Chapter 2.99 of the Berkeley Municipal Code.

FISCAL IMPACTS OF RECOMMENDATION

There are no fiscal impacts associated with adopting the attached resolution.

CURRENT SITUATION AND ITS EFFECTS

On March 27, 2018, the City Council adopted Ordinance 7,592-N.S., adding Chapter 2.99 to the Berkeley Municipal Code, which is also known as the Surveillance Technology Use and Community Safety Ordinance (“Ordinance”). The purpose of the Ordinance is to provide transparency surrounding the use of surveillance technology, as defined by Section 2.99.020 in the Ordinance, and to ensure that decisions surrounding the acquisition and use of surveillance technology consider the impacts that such technology may have on civil rights and civil liberties. Further, the Ordinance requires that the City evaluate all costs associated with the acquisition of surveillance technology and regularly report on their use.

The Ordinance imposes various reporting requirements on the City Manager and staff. The purpose of this staff report and attached resolution is to satisfy the annual reporting requirement as outlined in Section 2.99.070.

One of the reporting categories of the surveillance technology use is whether complaints have been received by the community about the various technologies. To date Berkeley Police Department Internal Affairs Bureau (IAB) has not received any external personnel complaints surrounding the use of Automatic License Plate Readers,

(Continued from January 25, 2022)

GPS Trackers, or Body Worn Cameras. External complaints from community members can be made in writing, via email, in person or via telephone. Complaints can be received with direct communication to Internal Affairs from the complainant and/or be received by any member of the Department and then forwarded through the chain of command. If a community member initiates a complaint against a subject employee and during the investigation it is determined the subject employee violated policy regarding the misuse of technology, an additional complaint is initiated by the Chief of Police.

Community members also have the right to initiate complaints against employees of BPD by reporting directly to the Police Accountability Board (PAB). The Director of Police Accountability notifies the Chief of Police when an investigation into a complaint is initiated by the PAB, which would prompt a parallel IAB investigation.

Attached to this staff report are Surveillance Technology Reports for Automatic License Plater Readers, GPS Trackers, Body Worn Cameras, and the Street Level Imagery Project.

#### BACKGROUND

On March 27, 2018, the City Council adopted Ordinance 7,592-N.S., adding Chapter 2.99 to the Berkeley Municipal Code, which is also known as the Surveillance Technology Use and Community Safety Ordinance. Section 2.99.070 of the Ordinance requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance at the first regular City Council meeting in November.

For each of the four technologies, the Surveillance Technology Reports were prepared to satisfy the specific, section-by-section requirements of the Ordinance, and are attached to this report.

The Surveillance Technology Use Policy for ALPR technology is still outstanding due Council questions about policy language, scheduling and directed focus during COVID-19. This item will be returned to the Council agenda in early 2022.

#### ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

There are no identifiable environmental effects or opportunities associated with the content of this report.

#### RATIONALE FOR RECOMMENDATION

City Council is being requested to adopt the attached resolution for the City to be in compliance with the Ordinance.

#### ALTERNATIVE ACTIONS CONSIDERED

City Council could decide not to adopt the resolution.

(Continued from January 25, 2022)

CONTACT PERSON

LaTanya Bellow, Interim Director of Information Technology (510) 981-6541

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

LaTanya Bellow, Interim Deputy City Manager, (510) 981-7012

ATTACHMENTS

1. Resolution
2. Body Worn Cameras
  - a) Surveillance Technology Report: Body Worn Cameras
  - b) Retention Schedule
3. Global Positioning System (GPS) Tracking Devices  
Surveillance Technology Report
4. Automated License Plate Readers  
Surveillance Technology Report: Automated License Plate Readers
5. Street Level Imagery Project  
Surveillance Technology Report: Street Level Imagery Project

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

A RESOLUTION ACCEPTING THE SURVEILLANCE TECHNOLOGY REPORT FOR AUTOMATIC LICENSE PLATE READERS, GPS TRACKERS, BODY WORN CAMERAS, AND THE STREET LEVEL IMAGERY PROJECT

WHEREAS, on March 27, 2018, the City Council adopted Ordinance 7,592-N.S., which is known as the Surveillance Technology Use and Community Safety Ordinance ("Ordinance"); and

WHEREAS, Section 2.99.070 of the Ordinance requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance at the first regular City Council meeting in November; and

WHEREAS, the Surveillance Technology Reports satisfy the requirements of the Ordinance.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the Council hereby accepts the Surveillance Technology Reports for Automatic License Plate Readers, GPS Trackers, Body Worn Cameras, and the Street Level Imagery Project.

**Surveillance Technology Report: Body Worn Cameras**

**October 1, 2020 – Sept. 30, 2021**

<p>Description</p>	<p>A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing.</p> <p>Body Worn Cameras are used to capture video recordings of contacts between department personnel and the public, to provide an objective record of these events. These recording are used in support of criminal prosecutions, to limit civil liability, increase transparency and enhance professionalism and accountability in the delivery of police services to the community. Body Worn Camera (BWC) files are shared with the Alameda County District Attorney’s office in support of prosecution for crime, and may be shared with other law enforcement agencies to support criminal investigations.</p> <p><b>Policy regarding activation of the Body Worn Camera BPD Policy 425.7</b></p> <p>Members shall activate the BWC as required by this policy in (a)-(f) below, and may activate the BWC at any time the member believes it would be appropriate or valuable to record an incident within the limits of privacy described herein.</p> <p>The BWC shall be activated in any of the following situations:</p> <ul style="list-style-type: none"> <li>(a) All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.</li> <li>(b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.</li> <li>(c) Self-initiated field contacts in which a member would normally notify the Communications Center.</li> <li>(d) Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence.</li> <li>(e) Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording.</li> <li>(f) Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.</li> </ul> <p><b>What data is captured by this technology:</b></p> <p>BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy. Improper use or release of BWC</p>
--------------------	---

recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited.

**How the data is stored:**

BWC videos are stored on a secure server. All BWC data will be uploaded and stored on Axon Cloud Services, Evidence.com. Axon complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States (collectively, "Privacy Shield"). Axon has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles.

**Retention period of data:**

See attached retention schedule.

Summary of Body Worn Camera Videos Uploaded Oct. 1, 2020 to Sept. 30, 2021:

Total Number of Videos	62,283
Total Hours of Videos	16,310
Total GB of BWC Videos	29,017

Summary of Digital Evidence Uploaded, Oct. 1, 2020 to Sept. 30, 2021:

Type	File Count	Size (GBs)
Audio	1,150	11.72
Document	737	2.38
Image	67,672	331.36
Other	1,292	157.71
Video*	67,865	30,086.75
<b>Total</b>	<b>138,716</b>	<b>30,589.92</b>

\* Includes all uploaded BWC videos and all other videos booked into the evidence management system. Other videos include iPhone videos uploaded, security camera video, copies of BWC videos (for redaction, etc.), and any other videos.

<p><b>Geographic Deployment</b></p>	<p>Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically.</p> <p>Body Worn Cameras are worn by all BPD uniformed officers city-wide at all times; BWCs are not deployed based on geographic considerations.</p>
<p><b>Complaints</b></p>	<p>A summary of each complaint, if any, received by the City about the Surveillance Technology.</p> <p>There have been no complaints about the deployment and use of Body Worn Cameras.</p>
<p><b>Audits and Violations</b></p>	<p>The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response.</p>

	<p>File meta-data are routinely reviewed by our BWC manager, to ensure required metadata fields are completed. There have been no complaints with regards to violations of the Surveillance Use Policy.</p>
Data Breaches	<p>Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.</p> <p>There have been no known data breaches or other unauthorized access to BWC data.</p>
Effectiveness	<p>Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes.</p> <p>Body Worn Cameras have proven effective in supporting criminal prosecutions, as video footage is available for all criminal prosecutions. Body Worn Cameras have been effective for training purposes, as footage can be reviewed in incident de-briefs. Body Worn Cameras have been extremely effective in support of Internal Affairs investigations and Use of Force Review.</p>
Costs	<p>Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.</p> <p>The annual cost for the Body Worn Cameras, including cameras, replacement cameras, software, and Axon's secure digital evidence management system is approximately \$204,000 per year over a five-year, \$1,218,000 contract. There is one full-time employee assigned to the BWC program, an Applications Programmer Analyst II, at a cost of \$168,940 per year, including benefits.</p>

NAME	RETENTION DURATION
Uncategorized	Until manually deleted
187 / Felony Sex Assault	Until manually deleted
Civil / City / Non-Evidence	1 year
Collision	2 years
Consent / Aid	108 weeks
Detention / Warrant Only	108 weeks
Felony Evidence	5 years
Litigation	Until manually deleted
Misdemeanor Evidence	2 years
Officer Injury	Until manually deleted
OIS / Critical Incident	Until manually deleted
Pending Review	Until manually deleted
Personnel / VSA	3 years
Personnel Complaint	Until manually deleted
Traffic Stop	108 weeks
Training	60 days
Use of Force	108 weeks
z_Saved	Until manually deleted



## Surveillance Technology Report: Global Positioning System Tracking Devices

October 1, 2019 – Sept. 30, 2020

Description	<p>A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing.</p> <p>Global Positioning System Trackers are used to track the movements of vehicles, bicycles, other items, and/or individuals.</p> <p><b>What data is captured by this technology:</b> A GPS Tracker data record consists of date, time, latitude, longitude, map address, and tracker identification label. The data does not contain any images, names of subjects, vehicle information or other identifying information on individuals.</p> <p><b>How the data is stored:</b> The data from the GPS tracker is encrypted by the vendor. The data is only accessible through a secure website to BPD personnel who have been granted security access.</p> <p><b>Retention period of data:</b> Tracker data received from the vendor shall be kept in accordance with applicable laws, BPD policies that do not conflict with applicable law or court order, and/or as specified in a search warrant.</p> <p>For the date range of 10-01-19 through 09-30-20 the Global Positioning System (GPS) “Electronic Stake Out” (ESO) devices were deployed on “bait” bicycles 52 times, resulting in 34 arrests, 4 eluded capture, 1 person was detained and not arrested, and in 13 deployments the bicycle was not stolen. This program was suspended in mid-March due to the COVID-19 pandemic.</p> <p>GPS “Slap-N-Track” (SNT) devices were used in three separate investigations during this reporting period:</p> <ul style="list-style-type: none"> <li>(1) An investigation of an individual for Sexual Exploitation, Child Pornography, and Distribution of Child Pornography. This suspect currently has a Federal warrant.</li> <li>(2) An investigation of a serial kidnap rape suspect. The suspect was arrested and charged.</li> <li>(3) An investigation into multiple suspects involved in a “Rolex” robbery series that involved the cities of Berkeley, Piedmont, and Orinda. Two devices were used on two different suspect vehicles during this investigation. Four suspects from the above cases were arrested and charged for their involvement in these robberies.</li> </ul>
-------------	---

	Data may be shared with the District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence; other law enforcement personnel as a part of an active criminal investigation; and other third parties, pursuant to a court order.
Geographic Deployment	<p>Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically.</p> <p>GPS ESO-equipped bikes were deployed primarily in commercial districts across the city where bikes are frequently stolen.</p> <p>GPS SNT devices are deployed with judicial pre-approval, based on suspect location, rather than geographical consideration.</p>
Complaints	<p>A summary of each complaint, if any, received by the City about the Surveillance Technology.</p> <p>There were no complaints made regarding GPS Trackers.</p>
Audits and Violations	<p>The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response.</p> <p>There were no audits and no known violations relating to GPS Trackers.</p>
Data Breaches	<p>Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.</p> <p>There were no known data breaches relating to GPS Trackers.</p>
Effectiveness	<p>Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes.</p> <p>GPS Trackers continue to be very effective in apprehending bicycle thieves, many of whom are repeat offenders who've committed not only bike thefts, but other crimes as well, such as burglaries, auto burglaries, and vehicle thefts. SNT trackers are effective in that they provide invaluable information on suspect vehicle location during the investigation of complex cases where suspects may be moving around the Bay Area and beyond.</p> <p>GPS Trackers greatly reduce costs associated with surveillance operations. A bike may be left for days. Surveillance operations generally involve four or more officers for the entire duration of an operation. A moving surveillance is extremely resource-intensive, requiring multiple officers in multiple vehicles for extended periods of time. Using both types of GPS trackers eliminates the need for officers' immediate presence until officers are ready to apprehend the suspect(s).</p> <p>The program was suspended in mid-March due to the COVID-19 pandemic. This program will likely resume once the pre-COVID bail schedule is re-established.</p>
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.

The annual cost for the GPS Trackers' data service is \$1,920. Further information regarding costs is contained in Policy 1301a, the Surveillance Acquisition Report.

There are staff time costs associated with preparing and placing SNT trackers. The investigator must prepare a search warrant and obtain a judge's approval, and a small number of officers must place the tracker on the suspect's car. The total number of hours is a fraction of the time it would take to do a full surveillance operation involving numerous officers.

There are staff time costs associated with preparing ESO trackers and placing ESO tracker-equipped bikes for bait bike operations. These are on the order of two-four hours per operation. The total number of hours is extremely small, given the large number of operations, and resulting arrests.

## Surveillance Technology Report: Automated License Plate Readers

October 1, 2019 – Sept. 30, 2020

Description	<p>A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing.</p> <p>Automated License Plate Readers (ALPRs) are used by Parking Enforcement Bureau vehicles for time zone parking and scofflaw enforcement. The City's Transportation Division uses anonymized information for purposes of supporting the City's Go Berkeley parking management program. ALPR use replaced the practice of physically "chalking" tires, which is no longer allowed by the courts.</p> <p><b>What data is captured by this technology:</b> ALPR technology functions by automatically capturing an image of a vehicle's license plate, transforming that image into alphanumeric characters using optical character recognition software, and storing that information, along with relevant metadata (e.g. geo-location and temporal information, as well as data about the ALPR).</p> <p><b>How the data is stored:</b> The data is stored on a secure server by the vendor.</p> <p><b>Retention period of data:</b> Collected images and metadata of hits are stored no more than 365 days. Metadata of reads are not stored more than 30 days.</p> <p style="text-align: center;"><b>Summary of ALPR Time Zone Enforcement Data</b></p> <p style="text-align: center;">Read Data There was an average of 12,059 "Reads" per working day (Based on one month's data: 9/1/20/-9/30/20)</p> <p style="text-align: center;">Hit Data There were 44,068 "Hits" 14,945 "Enforced Hits" resulted in citation issuance. 2,569 "Not Enforced" valid, enforceable hits resulted in no citation issued, based on PEO discretion.</p> <p>26,554 Hits were not acted upon for a variety of reasons including but not limited to:</p> <ol style="list-style-type: none"> <li>1) Customer comes out to move a vehicle. PEO's are directed not to issue that citation.</li> <li>2) Officer gets to the dashboard and sees a permit not visible from a previous location.</li> <li>3) Officer does a vehicle evaluation and confirms that the vehicle moved from the hit location (e.g. across the street within GPS range).</li> <li>4) Stolen car.</li> <li>5) Similar Plates.</li> <li>6) 600-700 GIG cars- 100 revel scooters.</li> </ol>
-------------	--

	<p>7) Officers leave their LPR “on” collecting time zone enforcement data, but leave the area being enforced to drive to another location on another assignment, such as a traffic post at a collision scene. These hits are not enforced.</p> <p>Genetec is the vendor for the ALPR Time Zone enforcement system. A “read” indicates the ALPR system successfully read a license plate. The information that is generated when a plate is viewed by the ALPR camera is the license plate number, state and geographical (GPS) location it was viewed. A “hit” indicates the ALPR system detected a possible violation, which prompts the Parking Enforcement Officer to further assess the vehicle. At “hit” is when the “read” information is recognized as a license plate that matches, or does not match an entry in a list such as permit list or the stolen vehicle “hot list”. In many cases, hits are “rejected” or “not enforced”, meaning no enforcement action is taken, because the Parking Enforcement Officer determines the vehicle has an appropriate placard or permit, or there is other information or assignment which precludes citation.</p> <p style="text-align: center;"><b>Summary of ALPR Booting Scofflaw Enforcement Data</b></p> <p style="text-align: center;">0 vehicles booted from 10/1/19-9/23/20.</p> <p>The Berkeley Police Department no longer maintains the ALPR Booting Scofflaw Enforcement Program. The contract to provide this service became cost prohibitive and the city opted not to renew the contract with the vendor. The city returned to having each PEO working a beat again become responsible for recognizing when a license plate has accumulated five or more unpaid parking tickets.</p> <p>All BPD ALPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes, or as otherwise permitted by law. All ALPR data is subject to the provisions of BPD Policy 415 - Immigration Law, and therefore may not be shared with federal immigration enforcement officials.</p>
<p><b>Geographic Deployment</b></p>	<p>Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically.</p> <p>Only Parking Enforcement Vehicles are equipped with ALPRs. ALPRs are deployed based on areas where there are parking time restrictions. ALPRs are not deployed based on geographic considerations not related to parking and scofflaw enforcement.</p>
<p><b>Complaints</b></p>	<p>A summary of each complaint, if any, received by the City about the Surveillance Technology.</p> <p>There have been no complaints about to the deployment and use of Automated License Plate Readers.</p>
<p><b>Audits and Violations</b></p>	<p>The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response.</p> <p>There have been no complaints of violations of the ALPR Surveillance Use Policy.</p>

<p>Data Breaches</p>	<p>Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.</p> <p>There have been no known data breaches or other unauthorized access to Automated License Plate Reader data.</p>
<p>Effectiveness</p>	<p>Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes.</p> <p>ALPRs have proven effective in parking enforcement for time zone enforcement; the prior utilization of manually chalking car tires for time zone enforcement has been disallowed by court decision.</p> <p>ALPRs have proven effective in supporting enforcement upon vehicles which have five or more unpaid citations. The ALPR's ability to read and check license plates while being driven greatly increases efficiency, allowing an operator to cover larger areas more quickly without having to stop except to confirm a hit.</p>
<p>Costs</p>	<p>Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.</p> <p>The annual system maintenance cost for Genetec is \$47,000. This cost is borne by the Transportation Division, which also purchased the ALPR units used in Time Zone Enforcement.</p> <p>Two new Genetec ALPR units were purchased during the period covered by this report. The two new units were purchased in order to equip the final two parking vehicles that did not have ALPR units attached to them.</p> <p>Genetec ALPR units are installed on 23 Parking Enforcement vehicles. Parking Enforcement personnel perform a variety of parking enforcement activities, and are not limited solely to time zone enforcement. Therefore, personnel costs specifically attributable to time zone enforcement are not tracked.</p>

## Surveillance Technology Report: Street Level Imagery Project

<p><b>Description</b></p>	<p><b>A description of all non-privileged and non-confidential information about the use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report will include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing.</b></p> <p>Street level imagery will be utilized exclusively by authorized City staff for infrastructure asset management and planning activities. The street level imagery of City infrastructure assets in the Public Right of Way that is provided to the City will not consist of information that is capable of being associated with any individual or group.</p>
<p><b>Geographic Deployment</b></p>	<p><b>Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically.</b></p> <p>Street level imagery was collected by driving through the entire community over a three week period. It is accessible to the City through a proprietary third-party application, Street SmartTM.</p>
<p><b>Complaints</b></p>	<p><b>A summary of each complaint, if any, received by the City about the Surveillance Technology.</b></p> <p>There have been no complaints about the deployment and use of Street SmartTM.</p>
<p><b>Audits and Violations</b></p>	<p><b>The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response.</b></p> <p>There have been no complaints with regards to violations of the Surveillance Use Policy.</p>
<p><b>Data Breaches</b></p>	<p><b>Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.</b></p> <p>There have been no known data breaches or other unauthorized access to Cyclomedia Street Level Imagery data.</p>





<p><b>Effectiveness</b></p>	<p><b>Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes.</b></p> <p>Staff considered hiring contractors to use GPS in the field to create and update the infrastructure asset GIS data. This method is costly and time consuming. Cyclomedia’s unique and patented processing techniques allow positionally-accurate GIS data to be collected in a cost-effective way and over a shorter period of time than a “boots on the ground” GPS field survey.</p> <p>The Imagery is being used to extract the following Citywide Infrastructure assets to create accurate and current Geographic Information Systems (GIS) data inventories:</p> <ul style="list-style-type: none"> <li>• Bus pads / stops</li> <li>• Maintenance Access Holes</li> <li>• Pavement Striping</li> <li>• Curb paint color</li> <li>• Parking meters</li> <li>• Pedestrian Signal</li> <li>• Pavement marking</li> <li>• Storm drains</li> <li>• Signs</li> <li>• Street trees</li> <li>• Traffic lights</li> </ul> <p>The street level imagery captured is also being used to:</p> <p>Create a street sign GIS layer with condition assessment to support compliance with the Manual on Uniform Traffic Control Devices Code and provide an accurate inventory of City signs. The existing sign inventory is contained in a spreadsheet that does not have accurate location data.</p> <p>Create a curb color layer with condition assessment to indicate where there are red, yellow, blue, white and green colors. This is critical to support Public Safety.</p> <p>Create pavement striping and paint symbol layers to support Transportation Planning and Vision Zero.</p> <p><b><u>Benefits Projected:</u></b></p> <p>The data from the street level imagery is being integrated into the City’s work order and asset management system for planning activities and to document repair and maintenance.</p> <p>Planners can use the street level imagery provided to the City to take measurements remotely, such as sidewalk width and public right of way impacts at proposed development locations.</p> <p>City staff can use the street level imagery to plan the location of road markings for pedestrian crossings, bike lanes or other striping.</p>
-----------------------------	--

	<p>City staff can remotely take accurate measurements of infrastructure assets to adequately plan for repair and replacement.</p> <p>City staff can use the street level imagery to enhance community engagement. The street level imagery can be used to identify and depict the impact of development such as an intersection restriping plan in order to article before and after conditions.</p>			
<b>Costs</b>	<p><b>Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.</b></p>			
	<p>The total cost of the system is \$232,401 and is itemized below.</p>			
	<b>Year No.</b>	<b>Description</b>	<b>Cost</b>	<b>Notes</b>
	1	Licenses	\$48,000	Resolution No: 69,482-N.S. 30JUN20
	1	Professional Services for asset extraction	\$139,401	Resolution No: 69,482-N.S. 30JUN20
	2	Licenses and Support – One-Time	\$45,000	Pending Council approval after imagery and data extraction work is completed Licensing Costs included in IT Cost allocation
3	License and Support – Ongoing Annual Costs	\$3,000	Pending Council approval after imagery and data extraction work is completed Licensing Costs included in IT Cost allocation	
<b>Total Year 1-3</b>		<b>\$235,401</b>		