Office of the City Manager

SUPPLEMENTAL AGENDA MATERIAL

for Supplemental Packet 2

Meeting Date: **November 12, 2019**

Item Number: **30**

Item Description: **Surveillance Technology Report, Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras**

Submitted by: **Dee Williams-Ridley, City Manager**

Attached is the originally published staff report with updated attachments. The staff report that was published did not include the surveillance technology reports. The following has been incorporated into the attachments:

- Surveillance Technology Report for Body Worn Cameras incorporated into Attachment 2.
- Surveillance Technology Report for Global Positioning System Tracking Devices incorporated into Attachment 3.
- Surveillance Technology Report for Automated License Plate Readers incorporated into Attachment 4.

2180 Milvia Street, Berkeley, CA 94704 Tel: 510.981.7000 TDD: 510.981.6903 Fax: 510.981.7099
E-Mail: *manager@CityofBerkeley.info*

Office of the City Manager

ACTION CALENDAR
November 12, 2019

To: Honorable Mayor and Members of the City Council

From: Dee Williams-Ridley, City Manager

Submitted by: Andrew Greenwood, Chief of Police
David White, Deputy City Manager

Subject: Surveillance Technology Report, Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras

RECOMMENDATION

Adopt a Resolution accepting the Surveillance Technology Report, Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras submitted 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 annual reporting requirements as outlined in sections 2.99.050 and 2.99.070. The attached Surveillance Technology Reports, Surveillance Acquisition Reports and Surveillance Use Policies for Automatic License Plater Readers, GPS Trackers, and Body Worn Cameras are for technologies that were acquired by the City prior to the adoption of the Ordinance.

Section 2.99.050 of the Ordinance required the City Manager to submit a Surveillance Acquisition Report and Surveillance Use Policy for each surveillance technology that has been possessed or used prior to the effective date of the Ordinance. The requirements of this section were not satisfied due to a multitude of factors, and the Police Department opted to submit the attached acquisition reports and use policies to the Police Review Commission prior to their review by the City Council. The Police Review Commission underwent an extensive engagement process and the full Commission discussed the attached use policies and reports at scheduled meetings from May to October 2019. In all cases, the Police Review Commission approved the attached acquisition reports and use policies and conveyed any concerns or suggested modifications to the Police Chief. In addition to the technologies covered by the attached resolution, City staff continues to evaluate whether or not there is any other technology that is used or possessed that is subject to the Ordinance.

Finally, Section 2.99.040 of the Ordinance allows the City Manager to borrow, acquire, or temporarily use surveillance technology in exigent circumstances without having to obtain the approval of City Council. Since the adoption of the ordinance, the City is reporting two instances in which the City Manager has made use of Section 2.99.040. In preparation for the potentially violent August 5, 2018 demonstration in downtown Berkeley, the City borrowed remote accessible cameras from the Northern California Regional Intelligence Center (NCRIC) in order to have the ability to remotely monitor intersections in real time. The cameras did not have face recognition technology. Signage was posted in the areas of the cameras, informing people that the area may be under video surveillance. Using cameras to monitor intersections is at times preferable to physically placing officers in those locations. In addition, as a mutual aid resource, the Police Department requested the Alameda County Sheriff's Office Small Unmanned Aerial System (sUAS) team as a mutual aid resource. The purpose of the request was to support the identification and apprehension of any felony suspects, should a felony occur. Following the felony vandalism of over ten City of Berkeley vehicles, the sUAS team deployed a drone, but no suspects were apprehended.

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. The Ordinance contains various reporting requirements including the following:

- Section 2.99.050, which requires that the City Manager shall submit a Surveillance Acquisition Report and a proposed Surveillance Use Policy for each technology governed by the Ordinance that had been possessed or used by the City prior to the effective date of the Ordinance; and

- Section 2.99.070 of the Ordinance, which 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 three technologies, the Surveillance Technology Report, Surveillance Acquisition Report and Surveillance Use Policies were prepared to satisfy the specific, section-by-section requirements of the Ordinance, and are attached to this report. It should be noted that substantial policies already existed for Body Worn Cameras and License Plate Readers. Those policies—also reviewed by the Police Review Commission for purposes of this report—are also attached. The existing policies will continue to remain in effect upon Council's approval. Henceforth, all new Surveillance Use Policies and Surveillance Acquisition Reports will be listed in Chapter 13 of the Berkeley Police Department Policy Manual, which is being created to provide easy access to all policies relating to BMC 2.99. All BPD policies are available to the public on BPD's website.

ENVIRONMENTAL SUSTAINABILITY

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

RATIONALE FOR RECOMMENDATION

City Council is being asked 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 or could direct staff to revise the attached policies.

CONTACT PERSON

Andrew Greenwood, Chief of Police, (510) 981-7017
David White, Deputy City Manager, (510) 981-7012

ATTACHMENTS

1. Proposed Resolution

2. Body Worn Cameras
   - Surveillance Technology Report: Body Worn Cameras
   - Policy 1300 Body Worn Camera Use Policy
   - Policy 1300(a) Appendix: Body Worn Camera Acquisition Report
   - Policy 425 Body Worn Camera Policy (Existing Policy)

3. Global Positioning System Tracking Devices
   - Surveillance Technology Report
   - Policy 1301 Global Positioning System Tracking Devices Use Policy
   - Policy 1301(a) Appendix: Global Positioning System Tracking Devices Acquisition Report

4. Automated License Plate Readers
   - Surveillance Technology Report: Automated License Plate Readers
   - Policy 1302 Automated License Plate Reader Use Policy
   - Policy 1302(a) Appendix: Automated License Plate Reader Acquisition Report
   - Policy 422 Automated License Plate Reader (Latest version of existing Policy)

5. Police Review Commission Memorandum Regarding Automatic License Plate Readers

i:\surveillance ordinance\city council meeting -- 11-12-19\11-12-2019_surveillance ordinance staff report and resolution (04).docx

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

A RESOLUTION ACCEPTING THE SURVEILLANCE TECHNOLOGY REPORT, SURVEILLANCE ACQUISITION REPORT, AND SURVEILLANCE USE POLICY FOR AUTOMATIC LICENSE PLATE READERS, GPS TRACKERS, AND BODY WORN CAMERAS

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 2.99.050 of the Ordinance requires that the City Manager shall submit a Surveillance Acquisition Report and a proposed Surveillance Use Policy for each piece of technology governed by the Ordinance that had been possessed or used by the City prior to the effective date of the 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 Acquisition Reports and Surveillance Use Policies for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras satisfy the requirements of the Ordinance.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley:

Section 1. Pursuant to Section 2.99.060, as it pertains to the use of Automatic License Plater Readers, GPS Trackers, and Body Worn Cameras, the City Council hereby finds and determines the following:

a. The benefits of using the technologies outweigh the costs;
b. The policies attached to this resolution safeguard civil liberties; and
c. No feasible alternatives exist with similar utility that will have a lesser impact on civil rights or liberties.

Section 2. The City Council hereby accepts the Surveillance Technology Reports, Surveillance Acquisition Reports, and Surveillance Use Policies for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras.

ATTACHMENT 2:
BODY WORN CAMERAS

Surveillance Technology Report: Body Worn Cameras

March 1, 2018 – Sept. 30, 2019

Description

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.

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 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.

Summary of Body Worn Camera Videos Uploaded
March 1, 2018 to Sept. 30, 2019

Total Number of Videos	42,677
Total Hours of Videos	10,681.93
Total GB of Videos	20,669.11

Summary of All Evidence Created
March 1, 2018 to Sept. 30, 2019

Type	Count of files	Size (in Mb)	GBs Storage
Audio	2,315	23,855.82	23.86
Document	125	17.56	0.02
Image	64,931	270,329.62	270.33
Other	896	118,080.19	118.08
Videos*	70,670	32,489,190.50	32,489.19
Grand Totals	138,937	32,901,473.69	32,901.47

* 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.

Geographic Deployment

Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically.

Body Worn Cameras are worn by all BPD uniformed officers city-wide at all times; BWCs are not deployed based on geographic considerations.

Complaints

A summary of each complaint, if any, received by the City about the Surveillance Technology.

There have been no complaints about the deployment and use of Body Worn Cameras.

Audits and Violations	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. File meta-data are routinely reviewed by our BWC manager, to ensure required meta-data fields are completed. There have been no complaints with regards to violations of the Surveillance Use Policy.
Data Breaches	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. There have been no known data breaches or other unauthorized access to BWC data.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. 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.
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The annual cost for the Body Worn Cameras, including cameras, replacement cameras, software, and Axon's secure digital evidence management system is approx. $204,000 per year over a five-year, $1,218,000 contract. The systems cost for the 19 month period of this initial report was $385,700. 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.

Surveillance Use Policy - Body Worn Cameras

1300.1 PURPOSE

This Surveillance Use Policy is issued in compliance with BMC 2.99, and incorporates by reference language from the Berkeley Police Department Body Worn Camera Policy #425 and adds elements as required by BMC 2.99.

The Berkeley Police Department recognizes that video recording of contacts between department personnel and the public provides an objective record of these events, and that the use of a recording system complements field personnel in the performance of their duties by providing a video record of enforcement and investigative field contacts, which can enhance criminal prosecutions, limit civil liability, increase transparency, and enhance professionalism in the delivery of police services to the community. A video recording of an event or contact also enables the delivery of timely, relevant, and appropriate training to maximize safety for both community members and BPD personnel. (Ref. policy 425.2)

1300.2 AUTHORIZED USE

This policy is not intended to describe every possible situation in which the BWC should be used. 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.

The BWC shall be activated in any of the following situations:

(a) All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.

(b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.

(c) Self-initiated field contacts in which a member would normally notify the Communications Center.

(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.

(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.

(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.

At no time is a member expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated by members in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the member can do so safely.

Members should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Members shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation. (Ref. policy 425.7)

1300.2.1 PROHIBITED USE

Members are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.

Members are prohibited from retaining BWC recordings. Members shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.

Recordings shall not be used by any member for the purpose of embarrassment, intimidation or ridicule. (Ref. policy 425.13)

1300.3 DATA COLLECTION

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 recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited. (Ref. policy 425.3)

1300.4 DATA ACCESS

Members are authorized to review their own BWC video files at any time in furtherance of official business. Such official business includes, but is not limited to, preparing written reports, prior to or while providing testimony in a case or being deposed. Members may review recordings as an evidentiary resource, except as stated in subsection 1300.4.1 below. Members shall not retain personal copies of recordings. Members shall not use the fact that a recording was made as a reason to write a less detailed report. (Ref. policy 425.17)

1300.4.1 OFFICER INVOLVED INCIDENTS RESULTING IN GRAVE BODILY INJURY OR DEATH

(a) In the event of a critical incident that results in grave bodily injury or death, including an officer-involved shooting or an in-custody death, the BWC of the involved member(s) shall be taken from him or her and secured by a supervisor, commander, or appropriate investigator, as necessary. The involved member(s) shall not access or obtain their footage of the incident until such time as the criminal investigator(s) have reviewed the video files.

It will be the responsibility of the investigation team's supervisor to coordinate with the involved member's supervisor to obtain footage of the incident on behalf of the member.

(b) Personnel uploading secured BWC video files shall not view the files unless authorized.

(c) No member involved in a critical incident may view any video recordings prior to an interview by the appropriate criminal investigative unit, and receiving command approval.

(d) Prior to the conclusion of the criminal interview process, the involved member and/ or the member's representative will have an opportunity to review the member's recording(s). The involved member may choose to provide additional information to supplement his or her statement by providing a supplemental statement or separate supplemental document. In no case shall a member alter a report made prior to reviewing the recording.

(e) The Department acknowledges that recordings taken during critical incidents obtained from BWCs do not necessarily reflect the full extent of the nature of the event or the experience, analysis, training, threat assessment or state of mind of the individual officers(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events recalled by the involved officer. Specifically, it is understood that the recording device will capture information that may not have been heard and/or observed by the involved officer and that officers may see and hear events that are not captured by the camera.

Officers who are involved in any critical incident where video recordings exist depicting the involved officer, either as a subject officer or witness, shall be provided the following admonishment to the initial interview or submission of the initial written report:

"In this case, there is video evidence that you will have an opportunity to view. Video evidence has limitations and may depict the events differently than you recall, and may not depict all of the events as seen or heard by you. Video has a limited field of view and may not capture events normally seen by the human eye. The "frame rate" of video may limit the camera's ability to capture movements normally seen by the human eye. Lighting as seen on the video may be different than what is seen by the human eye. Videos are a two-dimensional medium and may not capture depth, distance or positional orientation as well as the human eye. Remember, the video evidence is intended to assist your memory and ensure that your statement explains your state of mind at the time of the incident." (Ref. policy 425.17.1)

1300.4.2 SUPERVISORY REVIEW

With the exception of section 1300.4.1 above, supervisors are authorized to review relevant recordings any time they are reviewing and approving case reports from their subordinates. (Ref. policy 425.17.2)

1300.4.3 INVESTIGATORY REVIEW

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct, or whenever such recordings support review of the member's performance. (Ref. policy 425.17.3)

(a) Recorded files may also be reviewed:

1. Upon approval by a supervisor, by any member of the Department who is participating

in conduct of an official investigation, such as a personnel complaint, an administrative investigation or a criminal investigation.

2. Pursuant to lawful process or by court or District Attorney personnel who are otherwise authorized to review evidence in a related case.
3. By personnel assigned to investigatory units who are authorized to view any BWC video file associated to their active investigations, unless otherwise prohibited by policy.
4. Upon approval by the Chief of Police, Internal Affairs investigators may review BWC video with a complainant.

(b) Investigators conducting criminal or internal investigations shall:

1. Advise the coordinator to restrict access to the BWC file in criminal or internal investigations, as necessary.
2. Review the file to determine whether the BWC file is of evidentiary value and process it in accordance with established protocols.
3. Notify the coordinator to remove the access restriction when the criminal/internal investigation is closed.

1300.4.4 TEACHING OR LEARNING TOOL

BWC files may also be reviewed by training staff regarding specific incidents where such files may serve as an internal learning or teaching tool. In the event that videos are intended to be used for training purposes, the involved officer(s) will first be consulted. If he/she objects to the use of the video, such objection shall be submitted to the person in charge of training who shall weigh the value of the video for training against the officer(s) objections and basis for the objection. Should the person in charge of training refuse to grant the request of the involved officer(s), the matter shall be heard by the Chief of Police, or his/her designee, prior to utilizing the video. (Ref. policy 425.17.4)

1300.4.5 COB CIVIL CLAIMS AND LAWSUITS

BWC recordings may be reviewed and used by City of Berkeley defense counsel for the purposes of defending the city in civil claims and lawsuits, with the authorization of the Chief of Police, or his/her designee. (Ref. policy 425.17.5)

1300.5 DATA PROTECTION

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for uploading the data. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. (Ref. policy 425.14)

1300.6 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 BWC data. These policies will 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 potentially disparate or adverse impacts on any communities or groups.

1300.7 DATA RETENTION

The Department shall retain all recordings for a minimum of 60 days. Incidents involving consensual contacts, and aid to citizens will be retained for six months, and cold reports will be retained for one year. Recordings of incidents involving use of force by a police officer, detentions, arrests, or recordings relevant to a formal or informal complaint shall be retained for a minimum of two years and one month. Recordings relating to court cases and personnel complaints that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to administrative or civil proceedings shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court.

Recordings created by equipment testing or accidental activation may be deleted after 60 days. (Ref. policy 425.15)

1300.8 PUBLIC ACCESS

Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted under Government Code § 6254(f) and BPD General Order R-23 (Release of Public Records and Information). General Order R-23 does not authorize release of investigative files or documents that would constitute an unwarranted invasion of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy."

Access to recorded files will be granted for the purposes of review to media personnel or the general public with permission of the Chief of Police, or his/her designee, subject to General Order R-23 and privacy protections indicated in this policy. (Ref. policy 425.18)

1300.9 THIRD-PARTY DATA-SHARING

1300.9.1 CITY ATTORNEY

All recordings should be reviewed by the Custodian of Records and the City Attorney's Office prior to public release, see General Order R-23 (Release of Public Records and Information).

In the event that the Police Department or City Department intends to release or publish for any purpose video recordings where officers are captured on video or the video depicts actions taken by them in the course of the performance of their official duties, those officers shall be given written notice of the intention to release or publish said video at least 48 hours prior to such release.

BPD may, without prior notice to involved officers, share video footage with law enforcement, national security, military, or other government agencies outside of Berkeley, when there is reasonable suspicion that criminal activity has occurred or is about to occur. (Ref. policy 425.18)

1300.9.2 POLICE REVIEW COMMISSION (PRC)

Access to recorded files will be granted for the purposes of review to the Police Review Commission Officer and/or Investigator investigating a specific complaint where BWC evidence files are available, and are not part of any ongoing criminal investigation. (Ref. policy 425.18.1)

(a) The PRC Officer and PRC Investigator will be provided user account access to evidence files through the evidence management system for their use during a complaint investigation and to facilitate viewing by Board of Inquiry members during a Board of Inquiry.

(b) The PRC Officer and PRC investigator shall not make or create a copy of any evidence file, nor make or allow to be made any audio or video recording of any evidence file while it is being streamed and viewed from the evidence management system.

(c) The PRC Officer and PRC Investigator shall not allow any unauthorized individuals to view or access evidence files.

(d) The evidence management system associates an audit trail record with each evidence file, thereby logging the date, time, user, activity, and client IP address occurring during each evidence file access.

(e) The evidence management system shall only be accessed on City premises.

(f) The Department retains custody and control of the recordings, and content of the video will be subject to applicable legal standards including, but not limited to the confidentiality requirements of the Public Safety Officers' Procedural Bill of Rights, (Government Code § 3300, et seq., Penal Code § 832.7, and the California Public Records Act; Government Code § 6250, et seq.)

1300.10 TRAINING

Training for the operation of BWC's shall be provided by BPD personnel. All BPD personnel who use BWC's shall be provided a copy of this Surveillance Use Policy.

1300.11 AUDITING AND OVERSIGHT

Division Captains for divisions utilizing BWC's shall ensure compliance with this Surveillance Use Policy.

1300.12 MAINTENANCE

The BWC system will be maintained by the Applications Programmer Analyst and assigned

Department of Information and Technology (IT) staff.

The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code § 832.18) (Ref policy 425.4):

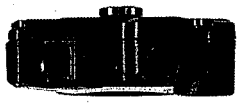
(a) Establishing a system for uploading, storing and security of recordings.
(b) Designating persons responsible for uploading recorded data.
(c) Establishing a maintenance system to ensure availability of BWCs.
(d) Establishing a system for tagging and categorizing data according to the type of incident captured.
(e) Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
(f) Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
(g) Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file, thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.
(h) All recordings made by members acting in their official capacity shall remain the property of the Department. Subject to the provisions of this Policy, members shall have no expectation of privacy or ownership interest in the content of these recordings.

BODY WORN CAMERAS (BWCs)

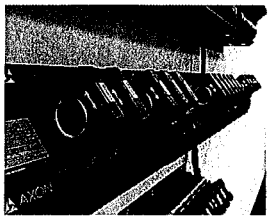
A. DESCRIPTION

The BWC system consists of four main components: The camera, the docking station, and the Digital Information Management System (DIMS) and smartphone applications.

The first component, the Axon camera, is a system which incorporates an audio and video recording device. It is designed to record events in real time for secure storage, retrieval, and analysis. The camera is to be attached to an officer's uniform and is powered by an internal rechargeable battery. The camera features low-light performance, full-shift battery life, a capture rate of 30 frames per second with no dropped frames, HD video, pre-event buffering, multi-camera playback, and the ability to automatically categorize video using the police department's computer aided dispatch system. An officer can start and stop recording by pressing a button on the front of the camera. The camera does not contain a screen for footage review.



The second component of the system is the docking station. Once the Axon camera is placed in the docking station it recharges the camera's battery. The dock also triggers the uploading of data from the camera to a cloud based Digital Information Management System (DIMS) called Evidence.com. The dock does not directly provide functionality to view, modify or delete video data stored on Axon cameras.



The third component is the Digital Information Management System called Evidence.com. Evidence.com streamlines data management and sharing on one secure platform. The evidence management system is comprehensive, secure, and intuitive to use. The DIMS is located in a cloud-based data center for security, scalability, and ease of administration. Users can add

metadata to existing videos such as associated case numbers, incident type, incident dispositions, etc. to make the videos easier to find. However, the videos themselves cannot be altered by the user.

The fourth component of the system to be utilized are two Axon mobile applications, which allow officers to collect and review evidence in the field and more effectively use their BWCs. The applications use secure Bluetooth and Wi-Fi technology to access the BWC systems and footage. These applications are compliant with US Department of Justice evidentiary standards, meaning that they are both secure and are set up in a way that prohibits the altering or destruction of evidence. The applications are called Axon View and Axon Capture. Axon View allows users to change their camera settings, view live video, and review and tag recorded videos while they are stored on the BWC. Recorded videos remain in the BWC's memory, and cannon be manipulated or deleted. Axon Capture allows officers to use their city-issued smartphone's camera and microphone to take photographs, and record audio and video, and to upload this data directly to Evidence.com. These applications do not allow users to alter, manipulate, or edit any of the footage recorded by the BWC. These applications use secure technology to add value and efficiency to the BWC program.

B. PURPOSE

The primary objective of the BWC system is to document officer contacts, arrests, and critical incidents. Video footage collected by the BWCs will be used as evidence in both criminal and administrative investigations. Video footage not relevant to any investigation will be discarded after a defined retention period.

In instances where the officer might be expected to take law enforcement action of any kind, the officer is expected to record the encounter for the benefit of both the officer and the member of the public.

1. The BWC shall be activated in any of the following situations:
    i. All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.
    ii. Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
    iii. Self-initiated field contacts in which a member would normally notify the Communications Center.
    iv. 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.

v. 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.
vi. 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.

At no time is an officer expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the user can do so safely.

Officers should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Officers shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation.

2. Prohibited uses of the BWC system include:
   i. Officers shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police, or his/her designee.
   ii. Officers are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.
   iii. Officers are prohibited from retaining BWC recordings.
   iv. Officers shall not duplicate or distribute such recordings, except for department business purposes.

C. LOCATION

Officers may use BWCs anywhere where officers have jurisdiction to operate as sworn officers, in accordance with BPD policy #425.

D. IMPACT

With the introduction of BWCs, officers record all enforcement contacts with the public. To that end, an officer could find themselves engaged in their lawful duties in both public and private areas. Additionally, due to the nature of law enforcement work, an officer may be required to engage in sensitive conversations with individuals of all ages, including children.

The right to maintain someone's anonymity versus the need to gain information to maintain public safety is of paramount concern. The Department recognizes that all people have a right to privacy and is committed to protecting and safeguarding civil rights by adhering to the

strictest requirements of both state and federal law concerning release of audio/video recordings.

E. MITIGATION

In order to minimize violations of privacy, BWC policy provides that:

1. Officers should record any incident they feel would be appropriate or valuable to document. The BWC policy shall require officers to activate the BWC under the criteria listed above.
2. Officers should not activate the BWC and/or use caution when entering a public locker room, changing room, restroom, doctor's or attorney's office, or other place where individuals unrelated to the investigation are present and would have a heightened expectation of privacy unless the officer is investigating criminal activity or responding to a call for service.
3. BWC use is limited to enforcement and investigative activates 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.
4. BWC footage will be retained or released in accordance with applicable state and federal law. Criminal defendants will have access to relevant BWC footage via the court discovery process.
5. Officers are prohibited from retaining BWC recordings, Officers shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.
6. Officers are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. Officers may request restriction and subsequent deletion of an accidental recording according to the BWC policy.
7. Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted by law and department policy. Department policy does not authorize release of investigative files or documents that would constitute an unwarranted invasions of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy

F. DATA TYPES AND SOURCES

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 litigations, and other proceedings protected by confidentiality laws and department policy.

The BWC collects video and audio recordings of events occurring in the user's presence. As each video is created, the system automatically stamps the video with the current date/time and the camera user's identity. The user has the option to add metadata manually to existing recordings after they are created. Such metadata may include but is not limited to:

1. Category of contact (from Department's defined list)
2. Disposition of contact (arrest, citation, etc.)
3. Associated case number

G. DATA SECURITY

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for transferring the data into the digital evidence management system. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings.

Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited. The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code Section 832.18) (Ref. policy 425.14):

1. Establishing a system for uploading, storing and security of recordings.
2. Designating persons responsible for uploading recorded data.
3. Establishing a maintenance system to ensure availability of BWCs.
4. Establishing a system for tagging and categorizing data according to the type of incident captured.
5. Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
6. Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
7. Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file,

thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.

H. FISCAL COST

In 2017, the Berkeley City Council approved a resolution authorizing a contract between BPD and Axon. Axon was chosen after a competitive Request for Proposal (RFP) process. The contract will not exceed $1,218,103 and includes the cost of 200 body worn cameras, charging stations, accessories, software licenses, training and unlimited storage for five years. The purchase also includes replacement cameras and charging stations during the third and fifth year of the contract.

There will be an annual cost of approximately $250,000 to the police department's budget for a staff person to administer the body worn camera program beginning in FY 2019.

I. THIRD PARTY DEPENDENCE AND ACCESS

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.

J. ALTERNATIVES

Officers rely primarily on traditional policing techniques to gather evidence related to criminal investigations such as speaking to witnesses and suspects, gathering information from observations, and using standard data aggregation systems. These methods will continue to be employed as primary investigative tools that will be supplemented by use of BWCs to document police activity.

BWC technology provides video and audio documentation of policing activity in addition to the oral and written statements of officers, victims, and witnesses. Alternatives to the use of BWCs would be vehicle-based cameras and/or not utilizing BWCs. However, BPD sees the use of BWCs as an integral strategy to strengthen police transparency, prevent and resolve complaints against the police by civilians, document police-public interaction, and promote the perceived legitimacy and sense of procedural justice that communities have about their departments. There is a broad consensus – among community leaders, the ACLU, the Department of Justice, the Berkeley Police Department, and elected officials – that body-worn cameras can be an important tool for improving the high-quality public service expected of police officers.

K. EXPERIENCE OF OTHER ENTITIES

Numerous police agencies have adopted BWCs as a tool to help combat crime, to reduce citizen complaints and to reduce use of force situations. Many departments have developed their own usage policies which may include standards for required officer use, supervisory review, storage and data retention standards, and internal and public access.

A report for the U.S. Bureau of Justice Administration, https://www.bja.gov/bwc/pdfs/14-005_Report_BODY_WORN_CAMERAS.pdf - pages 6-8, cites a 2013 Rialto, CA study that showed that the use of BWCs led to a 59 percent decrease in UOF and an 87.5 percent decrease in citizen complaints. Likewise, the Mesa, AZ report noted in "Impact" Section above also points to large decreases in UOF and citizen complaints.

The 2017 Police Body Worn Cameras: A Policy Scorecard, https://www.bwcscorecard.org/, provides an analysis of how scores of different police agencies have employed BWCs through a defined list of metrics.

Body Worn Cameras

425.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable Body Worn Cameras (BWCs) by members of this department while in the performance of their duties.

This policy does not apply to non-BWC evidence, including other methods of audio or video recordings, interviews or interrogations conducted at any Berkeley Police Department facility, authorized undercover operations, wiretaps or eavesdropping (concealed listening devices).

425.2 POLICY

The Berkeley Police Department recognizes that video recording of contacts between department personnel and the public provides an objective record of these events, and that the use of a recording system complements field personnel in the performance of their duties by providing a video record of enforcement and investigative field contacts, which can enhance criminal prosecutions, limit civil liability, increase transparency, and enhance professionalism in the delivery of police services to the community. A video recording of an event or contact also enables the delivery of timely, relevant, and appropriate training to maximize safety for both community members and BPD personnel.

While recordings obtained from BWCs provide an objective record of events, it is understood that video recordings do not necessarily capture all events, activities and information, or reflect the full experience of the individual member(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events as perceived and recalled by the involved member. Specifically, it is understood that the BWC will capture information that may not have been seen and/or heard by the involved member and that the involved member may see and hear information that may not have been captured by the BWC.

425.3 CONFIDENTIALITY AND PROPER USE OF RECORDINGS

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

425.4 COORDINATOR

The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code § 832.18):

(a) Establishing a system for uploading, storing and security of recordings.

(b) Designating persons responsible for uploading recorded data.

(c) Establishing a maintenance system to ensure availability of BWCs.

(d) Establishing a system for tagging and categorizing data according to the type of incident captured.

(e) Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.

(f) Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.

(g) Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file, thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.

All recordings made by members acting in their official capacity shall remain the property of the Department. Subject to the provisions of this Policy, members shall have no expectation of privacy or ownership interest in the content of these recordings.

425.5 MEMBER RESPONSIBILITIES

Prior to going into service, each uniformed member who is assigned to wear a BWC will be responsible for making sure that he or she is equipped with a BWC issued by the Department, and that the BWC is in good working order. If the BWC is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to his/her supervisor to permit the supervisor or other department employee to provide the member with a functioning BWC as soon as practicable. Uniformed members should wear the recorder in a conspicuous manner as prescribed by the Department, to provide a generally unobstructed camera view of contacts between members of the public and department members.

Members lawfully engaged in their duties as a police officer are not required to obtain consent from, or give notice to, members of the public, prior to recording with their BWC.

Upon the approval of the Chief of Police, or his/her designee, non-uniformed members lawfully engaged in their duties as a police officer may use an approved BWC.

Members are required to document the existence of a recording in any report or other official record of the contact, such as a CAD entry, including any instance where the member is aware that the BWC malfunctioned or the member deactivated the recording. In the event activity outlined in section 425.7 is not captured in whole or in part the member shall document this and explain in their report their understanding, if any, of why the footage was not captured in the recording.

425.6 SUPERVISOR RESPONSIBILITIES

At such time as the scene is considered secure and safe, the on-scene supervisor shall take immediate physical custody of involved officer's/officers' BWC when the device may have captured an incident involving an officer-involved shooting or use of force resulting in death or great bodily injury, and shall ensure the data is uploaded in a timely manner as prescribed by BPD policy

(Penal Code § 832.18). Supervisors may review relevant BWC video and audio files in the field in furtherance of their duties and responsibilities.

Supervisors shall also review relevant BWC recordings prior to submitting any administrative reports.

425.7 ACTIVATION OF THE BODY WORN CAMERA

This policy is not intended to describe every possible situation in which the BWC should be used. 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.

The BWC shall be activated in any of the following situations:

(a) All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.

(b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.

(c) Self-initiated field contacts in which a member would normally notify the Communications Center.

(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.

(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.

(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.

At no time is a member expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated by members in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the member can do so safely.

Members should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Members shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation.

425.8 VICTIMS AND WITNESSES OF CRIMES; INFORMANTS

In the event that an officer has the opportunity to record interviews of victims and witnesses of crimes, they shall consider the following:

(a) **Witnesses:** In the event a crime witness or a member of the community wishes to report or discuss criminal activity anonymously, officers have the discretion to not record. Members may offer to avert their camera to capture only audio during the interview, when doing so would facilitate obtaining the witness's recorded statement. In cases where a witness requests they not be recorded, and the member agrees not to record, members should record their request prior to turning the camera off. When a member is already recording, the member shall record their explanation for turning the camera off prior to doing so.

(b) **Victims:** Upon request by the victim, officers have the discretion to not record the interview. Members may offer to avert their camera to capture only audio during the interview, when doing so would facilitate obtaining the victim's recorded statement. In cases where a victim requests they not be recorded, and the member agrees not to record, members should record their request prior to turning the camera off. When a member is already recording, the member shall record their explanation for turning the camera off prior to doing so.

1. **Domestic Violence Victims**: Members should attempt to record interviews of domestic violence victims to facilitate future prosecution efforts and discourage later recanting of statements. Members should also record interviews with children who witness domestic violence, when the child is willing.

2. **Child Abuse and Sexual Assault Victims:** Members shall have the discretion to record, absent any request to not record the interview by victims, witnesses, or non-suspect parents of victims, during child abuse and/or sexual assault investigations.

(c) **Informants:** Members shall not activate their recorders when conducting an interview or engaging in a conversation with a confidential informant, unless needed as evidence.

Members have no obligation to advise a victim or witness that he or she is being recorded, but may do so at their discretion. When a victim or witness requests they not be recorded, members may consider their request (See Penal Code 632).

Members shall remain sensitive to the dignity of all individuals being recorded and exercise discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy concerns may outweigh any legitimate law enforcement interest in recording. Recording should resume when privacy concerns are no longer at issue unless the member determines that the circumstances no longer fit the criteria for recording.

Informal community interactions differ from "consensual encounters" in which members make an effort to develop reasonable suspicion to detain or probable cause to arrest. To strengthen relationships between police and citizens, members may use discretion regarding the recording of informal, non-enforcement related interactions with members of the community.

425.9 ACTIVATION IN CROWD CONTROL SITUATIONS

During crowd control, protest or mass arrest incidents, members shall use their BWCs consistent with this policy, or when directed by the Incident Commander. The Incident Commander shall document his or her orders to activate in an appropriate report (e.g. Operations Plan or After Action Report).

The limitations outlined in the Intelligence Procedures for First Amendment Activities Policy governing intelligence-gathering procedures for First Amendment activities, apply to the use of BWCs and other recording devices.

Video recording of individuals who are picketing or engaged in peaceful protest will be avoided unless the officer believes a violation of criminal law is occurring, may occur, or if the officer interacts with a participant or third party to the event, or a participant or third party initiates contact with the member.

425.10 SURREPTITIOUS USE OF THE BWC

Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police, or his/her designee.

Members are prohibited from using department-issued BWCs for non-work related personal activity. BWCs will not be activated in places where members have a reasonable expectation of privacy, such as workplace locker rooms, dressing rooms, members' private vehicles or restrooms.

425.11 CESSATION OF RECORDING

Once activated, the member may mute or deactivate their BWC at any time based on their discretion, in the following circumstances:

(a) Discussion of tactical or confidential information with other law enforcement personnel.

(b) Where members are on a perimeter or assigned to a static post where the member's direct participation in the incident is complete and they are not actively part of an investigation.

(c) If it is necessary to discuss issues or concerns with an employee, supervisor, doctor, nurse, or paramedic in private.

(d) In the member's judgment, a recording would interfere with his or her ability to conduct an investigation.

Decisions regarding the reason for muting or BWC deactivation shall be noted on the recording, or otherwise documented.

Members shall cease audio/video recording whenever necessary to ensure conversations are not recorded between a person in custody and the person's attorney, religious advisor or physician, unless there is explicit consent from all parties to the conversation. This does not apply to conversations with paramedics or EMTs during their response at a scene, and during transport.

425.12 EXPLOSIVE DEVICE

Many portable recorders, including BWCs and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

Members believing that the use of a BWC may detonate an explosive device may deactivate their BWC in such cases.

425.13 PROHIBITED USE OF BODY WORN CAMERAS

Members are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.

Members are prohibited from retaining BWC recordings. Members shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.

Members may not use personally owned recorders (e.g. personal cell phone) to document contacts unless exigent circumstances exist to warrant the use of personally owned recording devices. Regardless, if a member is using a department-issued BWC, and/or another recording device, members shall comply with the provisions of this policy, including retention and release requirements. In every event where members use any recording device aside from or in addition to their department-issued BWC, the member shall document and explain the use and the exigent circumstance in their police report (e.g. the BWC failed and evidence needed to be captured at that moment in time).

Recordings shall not be used by any member for the purpose of embarrassment, intimidation or ridicule.

425.14 PROCESSING AND HANDLING OF RECORDINGS

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for uploading the data. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. Members may request restriction and subsequent deletion of an accidental recording as described under section 425.16 below.

425.15 RETENTION REQUIREMENTS

The Department shall retain all recordings for a minimum of 60 days. Incidents involving consensual contacts, and aid to citizens will be retained for six months, and cold reports will be retained for one year. Recordings of incidents involving use of force by a police officer, detentions, arrests, or recordings relevant to a formal or informal complaint shall be retained for a minimum of two years and one month. Recordings relating to court cases and personnel complaints that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to administrative or civil proceedings shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court.

Recordings created by equipment testing or accidental activation may be deleted after 60 days.

425.16 ACCIDENTAL RECORDING - REQUEST FOR RESTRICTION

In the event of an accidental or sensitive personal recording of non-departmental business activity, where the resulting recording is of no investigative or evidentiary value, the recording employee may request that the file be restricted pending 60-day deletion by submitting an email request via their chain of command to the Professional Standards Division Captain. The Professional Standards Division Captain will approve or deny the restriction request. In cases where the request is denied, an appeal may be submitted to the Chief of Police, or his/her designee, for restriction authorization. In all cases of restriction requests, a determination should be made within seven calendar days.

425.17 REVIEW OF RECORDINGS BY A MEMBER

Members are authorized to review their own BWC video files at any time in furtherance of official business. Such official business includes, but is not limited to, preparing written reports, prior to or while providing testimony in a case or being deposed. Members may review recordings as an evidentiary resource, except as stated in subsection 425.17.1 below. Members shall not retain personal copies of recordings. Members shall not use the fact that a recording was made as a reason to write a less detailed report.

425.17.1 OFFICER INVOLVED INCIDENTS RESULTING IN GRAVE BODILY INJURY OR DEATH

(a) In the event of a critical incident that results in grave bodily injury or death, including an officer-involved shooting or an in-custody death, the BWC of the involved member(s) shall be taken from him or her and secured by a supervisor, commander, or appropriate investigator, as necessary. The involved member(s) shall not access or obtain their footage of the incident until such time as the criminal investigator(s) have reviewed

the video files. It will be the responsibility of the investigation team's supervisor to coordinate with the involved member's supervisor to obtain footage of the incident on behalf of the member.

(b) Personnel uploading secured BWC video files shall not view the files unless authorized.

(c) No member involved in a critical incident may view any video recordings prior to an interview by the appropriate criminal investigative unit, and receiving command approval.

(d) Prior to the conclusion of the criminal interview process, the involved member and/or the member's representative will have an opportunity to review the member's recording(s). The involved member may choose to provide additional information to supplement his or her statement by providing a supplemental statement or separate supplemental document. In no case shall a member alter a report made prior to reviewing the recording.

(e) The Department acknowledges that recordings taken during critical incidents obtained from BWCs do not necessarily reflect the full extent of the nature of the event or the experience, analysis, training, threat assessment or state of mind of the individual officers(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events recalled by the involved officer. Specifically, it is understood that the recording device will capture information that may not have been heard and/or observed by the involved officer and that officers may see and hear events that are not captured by the camera.

Officers who are involved in any critical incident where video recordings exist depicting the involved officer, either as a subject officer or witness, shall be provided the following admonishment to the initial interview or submission of the initial written report:

"In this case, there is video evidence that you will have an opportunity to view. Video evidence has limitations and may depict the events differently than you recall, and may not depict all of the events as seen or heard by you. Video has a limited field of view and may not capture events normally seen by the human eye. The "frame rate" of video may limit the camera's ability to capture movements normally seen by the human eye. Lighting as seen on the video may be different than what is seen by the human eye. Videos are a two-dimensional medium and may not capture depth, distance or positional orientation as well as the human eye. Remember, the video evidence is intended to assist your memory and ensure that your statement explains your state of mind at the time of the incident."

425.17.2 SUPERVISORY REVIEW

With the exception of section 425.17.1 above, supervisors are authorized to review relevant recordings any time they are reviewing and approving case reports from their subordinates.

425.17.3 INVESTIGATORY REVIEW
Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct, or whenever such recordings support review of the member's performance.

Recorded files may also be reviewed:

(a) Upon approval by a supervisor, by any member of the Department who is participating in conduct of an official investigation, such as a personnel complaint, an administrative investigation or a criminal investigation.

(b) Pursuant to lawful process or by court or District Attorney personnel who are otherwise authorized to review evidence in a related case.

(c) By personnel assigned to investigatory units who are authorized to view any BWC video file associated to their active investigations, unless otherwise prohibited by policy.

(d) Upon approval by the Chief of Police, Internal Affairs investigators may review BWC video with a complainant.

Investigators conducting criminal or internal investigations shall:

1. Advise the coordinator to restrict access to the BWC file in criminal or internal investigations, as necessary.
2. Review the file to determine whether the BWC file is of evidentiary value and process it in accordance with established protocols.
3. Notify the coordinator to remove the access restriction when the criminal/internal investigation is closed.

425.17.4 TEACHING OR LEARNING TOOL
BWC files may also be reviewed by training staff regarding specific incidents where such files may serve as an internal learning or teaching tool. In the event that videos are intended to be used for training purposes, the involved officer(s) will first be consulted. If he/she objects to the use of the video, such objection shall be submitted to the person in charge of training who shall weigh the value of the video for training against the officer(s) objections and basis for the objection. Should the person in charge of training refuse to grant the request of the involved officer(s), the matter shall be heard by the Chief of Police, or his/her designee, prior to utilizing the video.

425.17.5 COB CIVIL CLAIMS AND LAWSUITS
BWC recordings may be reviewed and used by City of Berkeley defense counsel for the purposes of defending the city in civil claims and lawsuits, with the authorization of the Chief of Police, or his/her designee.

425.18 RELEASE OF RECORDINGS

All recordings should be reviewed by the Custodian of Records and the City Attorney's Office prior to public release, see General Order R-23 (Release of Public Records and Information).

In the event that the Police Department or City Department intends to release or publish for any purpose video recordings where officers are captured on video or the video depicts actions taken by them in the course of the performance of their official duties, those officers shall be given written notice of the intention to release or publish said video at least 48 hours prior to such release.

BPD may, without prior notice to involved officers, share video footage with law enforcement, national security, military, or other government agencies outside of Berkeley, when there is reasonable suspicion that criminal activity has occurred or is about to occur.

425.18.1 POLICE REVIEW COMMISSION (PRC)

Access to recorded files will be granted for the purposes of review to the Police Review Commission Officer and/or Investigator investigating a specific complaint where BWC evidence files are available, and are not part of any ongoing criminal investigation.

(a) The PRC Officer and PRC Investigator will be provided user account access to evidence files through the evidence management system for their use during a complaint investigation and to facilitate viewing by Board of Inquiry members during a Board of Inquiry.

(b) The PRC Officer and PRC investigator shall not make or create a copy of any evidence file, nor make or allow to be made any audio or video recording of any evidence file while it is being streamed and viewed from the evidence management system.

(c) The PRC Officer and PRC Investigator shall not allow any unauthorized individuals to view or access evidence files.

(d) The evidence management system associates an audit trail record with each evidence file, thereby logging the date, time, user, activity, and client IP address occurring during each evidence file access.

(e) The evidence management system shall only be accessed on City premises.

(f) The Department retains custody and control of the recordings, and content of the video will be subject to applicable legal standards including, but not limited to the confidentiality requirements of the Public Safety Officers' Procedural Bill of Rights, (Government Code § 3300, et seq., Penal Code § 832.7, and the California Public Records Act; Government Code § 6250, et seq.)

425.18.2 PUBLIC RECORDS ACT (PRA) REQUEST

Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted under Government Code § 6254(f) and BPD General Order R-23 (Release of Public Records and Information). General Order R-23 does not authorize release of investigative files or documents that would constitute an unwarranted invasion of privacy.Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy."

425.18.3 MEDIA
Access to recorded files will be granted for the purposes of review to media personnel or the general public with permission of the Chief of Police, or his/her designee, subject to General Order R-23 and privacy protections indicated in this policy.

425.19 COMPLIANCE WITH BMC 2.99 ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

This policy shall comply at all times with the requirement of BMC 2.99 Acquisition and Use of Surveillance Technology.

425.20 TRAINING REQUIRED

Officers who are assigned BWCs must complete department-approved training in the proper use and maintenance of the devices before deploying to the field.

As part of a continual improvement process, regular review should be conducted by BPD staff of the training on this policy and the related use of BWCs under this policy. Information resulting from the outcomes of this review shall be incorporated into the City Manager's annual "Surveillance Technology Report" as required under BMC 2.99 Acquisition and Use of Surveillance Technology.

The Department, Police Review Commission and other City Departments shall maintain the confidentiality of Department sworn employee personnel records as required by state and local law. Failure to maintain the confidentiality of Department sworn employee personnel records, whether or not intentional, may subject individuals to civil penalties and discipline, up to and including termination of employment.

ATTACHMENT 3:
Global Positioning System Tracking Devices

Surveillance Technology Report: Global Positioning System Tracking Devices

March 1, 2018 – Sept. 30, 2019

Description	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. Global Positioning System Trackers are used to track the movements of vehicles, bicycles, other items, and/or individuals for the purpose of investigating criminal activity. Global Positioning System (GPS) "Electronic Stake Out" (ESO) devices were deployed on "bait" bicycles eighty-five (85) times during this reporting period, resulting in forty-nine (49) arrests. GPS "Slap-N-Track" (SNT) devices were used in two investigations during this reporting period: (1) a robbery and laptop snatch series involving multiple cases and suspects in Berkeley and in the region, with all suspects ultimately arrested; and (2) a currently-active case involving a series of auto burglaries in Berkeley and in the region. 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 investigations; and other third parties, pursuant to a court order.
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. GPS ESO-equipped bikes were deployed primarily in commercial districts across the city where bikes are frequently stolen. GPS SNT devices are deployed with judicial pre-approval, based on suspect location, rather than geographical consideration.
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. There were no complaints made regarding GPS Trackers.
Audits and Violations	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. There were no audits and no known violations relating to GPS Trackers.
Data Breaches	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. There were no known data breaches relating to GPS Trackers.

Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. 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. 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. 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).
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; the total cost for the 19 month period of this initial report was $3,040. 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 Use Policy - GPS Tracking Devices

1301.1 PURPOSE

Global Positioning System (GPS) tracking devices track the movements of vehicles, bicycles, cargo, machinery, other items, and/or individuals. GPS trackers electronically relay their precise location in real time, and thereby assist BPD in the recovery of evidence and arrest of suspects.

1301.2 AUTHORIZED USE

GPS trackers shall only be used during active criminal investigations. GPS trackers shall only be used pursuant to a lawfully issued search warrant, or with consent of the owner of the object to which the GPS tracker is attached.

GPS trackers shall only be utilized for law enforcement purposes.

1301.3 DATA COLLECTION

Location data may be obtained through the use of a GPS Tracker.

1301.4 DATA ACCESS

Access to GPS tracker data shall be limited to Berkeley Police Department (BPD) personnel utilizing the GPS Tracker(s) for active criminal investigations. Information may be shared in accordance with 1301.9 below.

In support of active criminal investigations, BPD personnel may receive GPS tracker data from probation or parole agencies which utilize GPS trackers (e.g. ankle monitors) as a condition of probation or parole.

1301.5 DATA PROTECTION

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.

1301.6 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. Provisions of this policy, including 1301.4 Data Access, 1301.5 Data Protection, 1301.7 Data Retention, 1301 .8 Public Access and 1301.9 Third Party Data Sharing serve to protect against any unauthorized use of GPS tracker data. These procedures 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 potentially disparate or adverse impacts on any communities or groups.

1301.7 DATA RETENTION

A GPS Tracker data record consists of date, time, latitude, longitude, map address, and tracker

identification label. This data is stored indefinitely by the vendor. The data does not contain any images, names of subjects, vehicle information, etc.

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.

1301.8 PUBLIC ACCESS

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law.

1301.9 THIRD-PARTY DATA-SHARING

Data collected from the GPS trackers may be shared with the following:

(a) The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
(b) Other law enforcement personnel as part of an active criminal investigation;
(c) Other third parties, pursuant to a Court Order.

1301.10 TRAINING

Training for the operation of the GPS trackers shall be provided by BPD personnel. All BPD personnel shall be provided with this Surveillance Use Policy.

1301.11 AUDITING AND OVERSIGHT

Division Captains or their designee shall ensure compliance with this Surveillance Use Policy.

1301.12 MAINTENANCE

GPS trackers shall only be obtained with the permission of the Investigations Division Captain or his/her designee. The Investigations Division Captain or his/her designee will ensure the trackers are returned when the mission/investigation is completed.

GPS TRACKING DEVICES

A. DESCRIPTION

Global Positioning System (GPS) tracking devices track the movements of vehicles, bicycles, cargo, machinery, other items, and/or individuals.

The Berkeley Police Department currently uses two types of GPS Tracking Devices to track the movements of vehicles, bicycles, or other kinds or property. The manufacturer, 3SI Security Systems, describes them as follows:

1. The "Slap-n-Track" (SNT) tracker tracks vehicles, cargo, and other large assets for long deployments. Offers extended battery life, rugged and weatherproof housing, and optional magnets.
2. The "Electronic Stake Out" (ESO) tracker offers Law Enforcement miniaturized and covertly packaged GPS Tracking Solutions to target property crimes, especially pattern crimes, in their local jurisdictions.

B. PURPOSE

Global Positioning System (GPS) tracking devices provide precise, real-time location information during the conduct of active criminal investigations. GPS trackers are only used pursuant to a lawfully issued search warrant, or with consent of the owner of the object to which the GPS tracker is attached.

C. LOCATION

GPS tracking devices shall be deployed in locations consistent with the authority granted by consent or a lawfully issued search warrant or court order.

D. IMPACT

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. GPS Trackers are used in place of expensive, resource-intensive surveillance operations which typically involve multiple officers, often over long periods of time. 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 utilized with GPS trackers help to ensure no unauthorized use of of GPS tracker data occurs. BPD Policy 1301 Surveillance Use Policy – GPS Tracking Devices ensure the use of GPS trackers and the resulting data are not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

E. MITIGATION

Data from a GPS tracker is encrypted from the vendor. Data shall be maintained in a secure, non-public location, such as locations requiring security access or badge access, thereby safeguarding the public from any impacts identified in subsection (D).

F. DATA TYPES AND SOURCES

A GPS tracker data record consists of date, time, latitude, longitude, map address (derived by using latitude, longitude and Google maps), and tracker identification label. The data does not contain any images, names of subjects, vehicle information, etc.

G. DATA SECURITY

Data from a GPS tracker is encrypted by the vendor on secure servers. The data is only accessible through a secure website to BPD personnel who have been granted security access. Captains whose Divisions utilize GPS trackers are responsible for ensuring compliance with the procedures for utilizing GPS Trackers.

H. FISCAL COST

The initial cost of the GPS trackers totaled $4,335.

- Between 2015-present BPD purchased 5 GPS "ESO" trackers for $2,250 ($450 each).
- In 2017 BPD purchased 3 GPS "SNT" trackers for $2,085 ($695 each).

The annual cost for the GPS data service totals $1,920.

- The annual data service for the five ESO trackers is $1,020 ($204 each).
- The annual data service for the three SNT trackers is $900 ($300 each).

Personnel costs are minimal in that the GPS trackers are used as a resource during normal working hours.

GPS trackers are funded through the Investigations Division's general budget.

I. THIRD PARTY DEPENDENCE AND ACCESS

Data collected from the GPS trackers may be shared with the following:

a. The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
b. Other law enforcement offices as part of a criminal investigation;
c. Other third parties, pursuant to a Court Order.

J. ALTERNATIVES

An alternative to the use of GPS trackers is to conduct resource-intensive surveillance operations utilizing numerous personnel over extended periods of time.

K. EXPERIENCE OF OTHER ENTITIES

The use of GPS tracker technology is common amongst law enforcement agencies throughout the country.

ATTACHMENT 4:
Automated License Plate Readers

Surveillance Technology Report: Automated License Plate Readers

March 1, 2018 – Sept. 30, 2019

Description	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. 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 GoBerkeley parking management program. ALPR use replaced the practice of physically "chalking" tires. **Summary of ALPR Time Zone Enforcement Data** Read Data There were an average of 9,075 "Reads" per working day (Based on one month's data: 9/9/19-10/9/19) Hit Data There were 69,738 "Hits" 18,410 "Enforced Hits" resulted in citation issuance. 51,328 "Not Enforced" Hits resulted in no citation issuance. (Based on one year's data: 10/9/18-10/9/19) Genetec is the vendor for the ALPR Time Zone enforcement system. A "read" indicates the ALPR system successfully read a license plate. A "hit" indicates the ALPR system detected a possible violation, which prompts the Parking Enforcement Officer to further assess the vehicle. In many cases, hits are "rejected" or "not enforced" because the Parking Enforcement Officer determines the vehicle has an appropriate placard or permit, or there is other information which precludes citation. **Summary of ALPR Booting Scofflaw Enforcement Data** 255 vehicles booted from 9/1/18-6/30/19 Paylock is the vendor for the ALPR Booting Scofflaw Enforcement Program. A single parking enforcement vehicle is equipped with the Paylock system ALPR. The Paylock ALPR system provides the operator a "hit" when a plate is recognized as having five or more unpaid parking tickets. The operator then further assesses the vehicle, confirms the citation data, and, if confirmed, creates a boot entry in Paylock, and boots the car. Paylock uploads and retains information to their secure server solely on *confirmed* boots or tows. Hits and reads are not retained in the Paylock server. Booting Scofflaw enforcement has been temporarily suspended due to the transition to a different citation management vendor.

	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.
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. 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.
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. There have been no complaints about the deployment and use of Automated License Plate Readers.
Audits and Violations	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. There have been no complaints of violations of the ALPR Surveillance Use Policy.
Data Breaches	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. There have been no known data breaches or other unauthorized access to Automated License Plate Reader data.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. ALPRs have proven effective in parking enforcement for time zone enforcement. 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.
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. 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. No Genetec LPR units were purchased during the period covered by this report. Genetec ALPR units are in use on 20 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.

	The cost of Paylock is $140 per boot. One Parking Enforcement Officer is assigned to scofflaw enforcement and abandoned auto enforcement on a full time basis. Assuming the Officer works approximately half their day on scofflaw enforcement, the annual personnel cost would be approximately one half a fulltime Parking Enforcement Officer's pay with benefits, or $65,000.

Surveillance Use Policy - ALPR

1302.1 PURPOSE

This Surveillance Use Policy is issued in compliance with BMC 2.99, and incorporates by reference language from the Berkeley Police Department ALPR Policy #422 and adds elements as required by 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 while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review. (Ref. policy 422.2)

1302.2 AUTHORIZED AND PROHIBITED USES USE

Use of an ALPR is restricted to the purposes outlined below. Department members 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). (Ref. policy 422.4)

(a) An ALPR shall only be used for official law enforcement business.

(b) An ALPR may be used to support a patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

1302.3 DATA COLLECTION

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law. (Ref. policy 422.5)

1302.4 DATA ACCESS

(a) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

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

(c) If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

1302.5 DATA PROTECTION

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53) (Ref. policy 422.6):

(a) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).

(b) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action and parking enforcement.

(c) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.

(d) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

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 potentially disparate or adverse impacts on any communities or groups.

1302.7 DATA RETENTION

The Investigations Division Captain, or his/her 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 Information Technology (IT) department and associated 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 CLETS information they are not authorized to receive. 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 ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence. (Ref. policy 422.5)

(a) Collected images and metadata of hits will not be stored for more than 365 days. Metadata of reads will not be stored for more than 30 days. Images of reads will not be transferred to the server.

1302.8 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. (Ref. policy 422.6 (a))

(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 requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question. (Ref. policy 422.6 (b))

1302.9 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 otherwise permitted by law. 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 shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager. (Ref. policy 422.6 (e))

1302.10 TRAINING

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.

1302.11 AUDITING AND OVERSIGHT

ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually. (Ref. policy 422.6 (g))

1302.12 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 his/her command to administer the day-to-day operation of the ALPR equipment and data. (Ref. policy 422.3)

1302.12.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply 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) (Ref.

policy 422.3.1):

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

(b) Training requirements for authorized users.

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

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

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

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

AUTOMATED LICENSE PLATE READER (ALPR) DEVICES

A. DESCRIPTION

Automated License Plate Readers (ALPRs) are high-speed, computer controlled camera systems that are typically mounted on Berkeley Police Department Parking Enforcement Vehicles.

ALPRs capture license plate numbers which come into view, along with the location, date and time. The data, which includes a photo of the front or the back of the car displaying the license plate, is then uploaded to a central server.

B. PURPOSE

The Berkeley Police Department's Parking Enforcement Unit utilizes vehicles equipped with ALPRs to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's also access information in the California Law Enforcement Telecommunications System's (CLETS) Stolen Vehicle System (SVS) database, which provides information on matches for stolen and wanted vehicles.

The Berkeley Police Department's Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates, and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding parking citation fees.

C. LOCATION

Parking Enforcement vehicles travel throughout the city; using the ALPRs as described above.

D. IMPACT

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 utilized with ALPR Units will help to ensure unauthorized use of its data. The procedures will 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 potentially disparate or adverse impacts on any communities or groups.

E. MITIGATION

All saved data will be safeguarded and protected by both procedural and technological means which are implemented to safeguard the public from any impacts identified in subsection (D). See subsection (G) for further.

F. DATA TYPES AND SOURCES

Photographs of license plates and location data may be obtained through the use of ALPR Units.

G. DATA SECURITY

The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

1. All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
2. Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action and parking enforcement.
3. Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
4. Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

H. FISCAL COST

In 2015, Public Works brought an ALPR Contract to City Council. Council approved a contract for Public Works to buy five Genetec ALPR Units with PCS Mobile communication, for a pilot program for $450,000.

In 2017, after success with the program, City Council approved an amendment to the contract, allowing Public Works to purchase 15 more ALPR Units for Parking Enforcement vehicles, and to continue its use of PCS Mobile, for 1,200,000. The money was allocated from the goBerkeley/Federal Highway Administration Parking Meter Fund.

Yearly service for the ALPR Units includes warranties, hosting services, cellular connection, mobile computing, and training which varies. The costs through fiscal year 2022 are currently estimated at $1,175,000.

Personnel costs are minimal in that the ALPR Units are used as a resource during normal working hours.

I. THIRD PARTY DEPENDENCE AND ACCESS

1. Vendor Access-Scofflaw Enforcement: The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:

    a. All data captured by the ALPR is stored on the booting vehicle's laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.

    b. When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.

2. Vendor Access-General Parking Enforcement and goBerkeley Program: The contracted vendor for the City's Parking Enforcement ALPR is currently Genetec. The city uses Genetec ALPRs to support efficient enforcement of posted time limit parking and Residential Preferential Parking permits.

    a. In addition, Genetec periodically provides reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that the City's program can analyze data about parking demand. These reports do not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports consist of completely anonymized information, using identification numbers that are not associated with a particular license plate or registered owner.

    b. The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and Residential Permit Pass (RPP) area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.

3. Department of Information Technology Access: Technical support and assistance for ALPR's is provided by the City of Berkeley's Department of Information Technology (IT) and associated ALPR system providers/vendors as identified herein. IT staff who

do not have the proper clearance and training do not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT provides initial infrastructure set-up, and continued systems support as needed to ensure efficient and accurate performance of the ALPR hardware and software. Only IT staff members who have successfully undergone DOJ background checks and training are authorized by the Chief of Police to view specific ALPR records.

4. Other Law Enforcement Agency Access: ALPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. 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 shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.

5. Member Access: No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training. No ALPR operator may access CLETS data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through CLETS before taking enforcement action that is based solely on an ALPR alert.

6. Public Access: 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. 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 requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

J. ALTERNATIVES

None.

K. EXPERIENCE OF OTHER ENTITIES

The use of ALPR technology is common amongst law enforcement agencies throughout the country, in support of parking enforcement, and law enforcement criminal investigations.

Automated License Plate Readers (ALPRs)

422.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

422.2 POLICY

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

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

422.3 ADMINISTRATION

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 his/her command to administer the day-to-day operation of the ALPR equipment and data.

422.3.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply 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):

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

(b) Training requirements for authorized users.

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

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

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

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

422.4 USE OF THE ALPR

An ALPR shall only be used for official law enforcement business.

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

(a) An ALPR may be used by Berkeley Police Department Parking Enforcement for parking and scofflaw enforcement.

(b) An ALPR may be used to support criminal investigations. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert

422.5 .DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review.

The Investigations Division Captain, or his/her 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 Information Technology (IT Department and associated 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 CLETS information they are not authorized to receive. 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 ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

(a) Collected images and metadata of reads showing violations will not be stored for more than 365 days.

(b) Metadata of reads showing violations will be stored for up to 30 days. Images of reads not

showing violations will not be transferred to the server.

422.6 ACCOUNTABILITY

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(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 requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

(c) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).

(d) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action or parking enforcement.

(e) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.

(f) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

(g) ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually.

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

422.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

4. The related case number.

(b) The request is reviewed by the Investigations Division Captain, or his/her designee, and approved before the request is fulfilled.

(c) The approved request is retained on file.

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).

ALPR data is subject to the provisions of the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

422.8 SCOFFLAW ENFORCEMENT

The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for parking and scofflaw enforcement.

The Parking Enforcement Unit will utilize vehicles equipped with ALPR units to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's will also access information in the DMV's Stolen Vehicle System (SVS) database for wanted and stolen vehicles.

The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding citation fees.

The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website.

When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.

The City's Parking Enforcement ALPR vendor (currently Genetec) will periodically provide reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that it can analyze data about parking demand. These reports will not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports will consist of 100 percent anonymized information using identification numbers that are not associated with a particular license plate or registered owner.

The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and RPP area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking

enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.

ATTACHMENT 5:
Police Review Commission Communication

Police Review Commission (PRC)

September 11, 2019

To: Honorable Mayor and Members of the City Council

From: George Perezvelez, Chairperson, Police Review Commission

Re: Proposed Berkeley Police Department Policy 422, Automated License Plate Readers

Summary: This memo is to inform you of the Police Review Commission's qualified approval of the BPD's proposed policy for the use of Automated License Plate Readers (ALPRs).

Background: The BPD submitted the ALPR policy, Policy 422, to the PRC for review, along with the Surveillance Use Policy and the Surveillance Acquisition Report (Policy 1302 and Appendix A) for these devices. This process was undertaken in advance of BPD submitting these items to the City Council as required by the Surveillance Technology Use and Community Safety Ordinance (B.M.C. Ch. 2.99).

These policies were first considered by the full Commission, which then referred them to its Lexipol Policies Subcommittee. In response to feedback from the PRC and the Subcommittee, the BPD revised the proposed policy, which was reviewed by both bodies. At various stages, the PRC and the subcommittee had the opportunity to hear from and ask questions of Police Chief Greenwood and other members of the BPD, and Deputy City Attorney Chris Jensen, The PRC also heard input from representatives of Media Alliance and Oakland Privacy.

Final action: At its September 4, 2019 meeting, the PRC voted to approve for submission to the City Council for your review and discussion the version of Policy 422 that is attached here, with two caveats. First, there was concern among some commissioners that the ALPR was originally acquired for the purpose of parking enforcement and that this policy represents an expansion of that function. If this is not what the Council had in mind, then this policy should be modified accordingly. Second, Section 422.4(c) of the policy does not adequately define what constitutes a "crime scene."

Finally, the Commission wishes to remind the Council that they will see actual use of the ALPR technology under the reporting mechanism in place in the Surveillance Technology Use and Community Safety Ordinance.

1947 Center Street, 1st Floor, Berkeley, CA 94704 Tel: 510-981-4950 TDD: 510-981-6903 Fax: 510-981-4955
e-mail: prc@cityofberkeley.info website: www.cityofberkeley.info/prc/

The above action was approved by the following vote: Moved/Seconded (Perezvelez/Mikiten) -- Ayes: Calavita, Chang, Leftwich, Mikiten, Perezvelez, Ramsey; Noes: Earnest, Mizell; Abstain: Allamby; Absent: None.

Attachment: Revised Policy 422

cc: Dee Williams-Ridley, City Manager
Andrew Greenwood, Chief of Police
David White, Deputy City Manager
PRC Commissioners

Automated License Plate Readers (ALPRs)

422.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

422.2 POLICY

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

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

422.3 ADMINISTRATION

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 his/her command to administer the day-to-day operation of the ALPR equipment and data.

422.3.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply 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):

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

(b) Training requirements for authorized users.

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

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

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

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

422.4 USE OF THE ALPR

An ALPR shall only be used for official law enforcement business.

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

(a) An ALPR may be used by Berkeley Police Department Parking Enforcement for parking and scofflaw enforcement.

(b) An ALPR may be used to support criminal investigations. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

422.5 DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ~~ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law.~~

The Investigations Division Captain, or his/her 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 Information Technology (IT Department and associated 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 CLETS information they are not authorized to receive. 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 ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

(a) Collected images and metadata of reads showing violations will not be stored for more than 365 days.

(b) Metadata of reads showing violations will be stored for up to30 days. Images of reads not showing violations will not be transferred to the server.

422.6 ACCOUNTABILITY

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(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 requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

(c) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).

(d) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action or parking enforcement.

(e) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.

(f) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

(g) ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually.

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

422.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.

2. The name of the person requesting.
3. The intended purpose of obtaining the information.
4. The related case number.

(b) The request is reviewed by the Investigations Division Captain, or his/her designee, and approved before the request is fulfilled.

(c) The approved request is retained on file.

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).

ALPR data is subject to the provisions of the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

422.8 SCOFFLAW ENFORCEMENT

The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for parking and scofflaw enforcement.

The Parking Enforcement Unit will utilize vehicles equipped with ALPR units to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's will also access information in the DMV's Stolen Vehicle System (SVS) database for wanted and stolen vehicles.

The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding citation fees.

The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:

(a) All data captured by the ALPR is stored on the laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.

When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.

The City's Parking Enforcement ALPR vendor (currently Genetec) will periodically provide reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that it can analyze data about parking demand. These reports will not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated

with a particular vehicle. Rather, the reports will consist of 100 percent anonymized information using identification numbers that are not associated with a particular license plate or registered owner.

The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and RPP area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.