

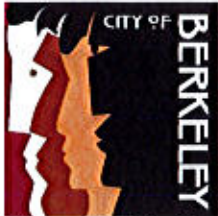
**PRC COMPLAINT DEADLINES REPORT**

COMPLAINT INVESTIGATIONS										
NO.	Complaint	Filed Date	Incident Date	Notice of Allegations Due (20 Bus. Day)	Notice of Allegations Issued	BOI Packet (80 days)	BOI Packet Issued	BOI Findings Report Goal (105 days)	120 Days	STATUS
2419		06/14/17	Jun-17	07/12/17	06/19/17	09/02/17		09/27/17	10/12/17	On hold; ofc unavail. no earlier than 7/10/19
2454		06/04/19	Jun-19	07/02/19	06/11/19	08/23/19		09/17/19	10/02/19	Admin Closure Rec to Commission 7/10
2456		06/24/19	Jun-19	07/22/19		09/12/19		10/07/19	10/22/19	Admin Closure Rec to Commission 7/24
2457		06/28/19	?	07/26/19		09/16/19		10/11/19	10/25/19	Comp interview due

BOARD OF INQUIRY APPEALS (CALOCA)										
NO.	Complaint	Officer Appeal Filed	PRC Records Due (60 d)	PRC Records Filed	Officer Brief Due	PRC Brief Due	PRC Brief Filed	OAH Hearing Date	OAH Decision Due	STATUS
2446		3/22/19	5/21/19	5/17/19	7/2/19	7/16/19		7/30/2019	09/27/19	PRC Brief Due

POLICY COMPLAINTS								
NO.	Complaint	Filed Date	Notice of Complaint to BPD	Due to Comm (30 days or next mtg.)	Initial Commission Meeting Date	Commission Approval Date	Commission Resolved? y/n	STATUS
2455	WILLIAMS, ELAINE	06/20/19	6/21/19	07/10/19	07/10/19			pending commission decision





Office of the City Manager

## **SUPPLEMENTAL AGENDA MATERIAL For Supplemental Packet 2**

**Meeting Date:** July 9, 2019

**Item Number:** 18b

**Item Description:** **Companion Report: Law Enforcement Use of Restraint Devices in the City of Berkeley**

**Submitted by:** **Andrew R. Greenwood, Chief of Police**

This supplemental material includes the most recent (July 5, 2019) draft of BPD Policy 302, as well as information and outcomes reflecting the extensive collaborative policy review process between the Police Review Commission and the Berkeley Police Department on this matter.

Policy 302 "Handcuffing and Restraints" provides policy for the safe use of handcuffs and other restraints during detentions and arrests.

The Police Review Commission (PRC) Lexipol Sub-Committee reviewed and provided input to Policy 302 in fall 2018. Several changes were made, and in October 2018, the policy was issued to the Department.

In considering the recent Mental Health Commission's item to Council, as well as the companion report, the PRC asked the Department to make a presentation regarding the use of spit hoods.

On June 12, 2019, BPD made a presentation to the full PRC, which can be viewed here: [https://youtu.be/uU\\_VXxUdqyl](https://youtu.be/uU_VXxUdqyl), starting at the 1:50:35 mark. In the ensuing discussion, the PRC raised concerns which had been discussed during the subcommittee meeting immediately prior to the June 12 full commission meeting. We discussed those issues during the PRC meeting.

On June 14, 2019, BPD responded to the PRC's input, returning a draft policy which addressed the concerns raised during the discussion, changing two instances of "should" to "shall" and strengthening language regarding medical concerns.

On June 18, 2019, the subcommittee discussed the draft as amended, and discussion continued at the June 26 meeting of the full commission.

On June 26, 2019, after substantial discussion, the full PRC passed a motion comprised of five elements. Please see below for our response on each element:

The PRC has voted to recommend approval of Policy 302 as follows:

1) In the second paragraph of Section 302.10, change the word "when" to "while" [so the sentence begins, "Spit hoods may be placed upon persons in custody while the officer reasonably believes...];

**Response:** The attached policy incorporates the substitution of "while" for "when", in section 302.10, second paragraph: "Spit hoods may be placed upon persons in custody **while** the officer reasonably believes the person will bite or spit..."

Based on input from the commission, though not a part of the PRC's motion, we have added language regarding trauma in the first paragraph of Section 302.10: "As the Department recognizes that use of a spit hood **may be experienced as a traumatic event to the wearer, and** may cause alarm and concern to onlookers, this policy provides clear and specific guidelines for their use, in service of the safety of all parties involved."

2) that the PRC endorses the BPD's commitment to crisis intervention training (CIT) and de-escalation strategies, and promotes the use of CIT officers in their application of spit hoods when practical.

**Response:** Berkeley PD continues its years-long, ongoing commitment to CIT training. BPD continues to send staff to fill each available training slot to the full week course. The majority of BPD officers have had CIT training. While this makes it likely a CIT-trained officer may be present when spit hoods are used, officers will not be prohibited by this policy from using a spit hood simply because a CIT-trained officer is not present.

3) that the Chief propose data collection measures for the PRC's consideration, including the types of circumstances hoods are used under.

**Response:** BPD is examining options to capture the number of times a spit hood (and the "Wrap" device as well) is used. It should be noted that according to this policy, spit hoods are *only* to be used "when the officer reasonably believes the person will bite or spit, either on a person or in an inappropriate place." Absent the officer's reasonable belief, spit hoods may not be applied. Body Worn Camera footage will support examination of any circumstances wherein a complaint is raised.

4) that the BPD utilize other available methods of restraint when possible, such as placing a person in a vehicle;

**Response:** Spit hoods are specifically designed to address the unique health and safety issues created by a person spitting or biting. Placement in a vehicle

is not a substitute for the proper utilization of a spit hood, when a subject is spitting and the officer reasonably believes the behavior will continue.

5) the use of spit hoods on pre-adolescent children is prohibited.

**Response:** There was substantial discussion of this issue with the PRC. We were unable to determine specific, clear definitional policy language on what "pre-adolescent" or similar terms mean in the context of a policy.

There is a de facto prohibition of the use of a spit hood on a small child within existing policy language.

Section 302.7 prohibits the use of any restraints on juveniles, (defined as persons "under 14 years old") unless the person "is suspected of a dangerous felony or when the officer has a reasonable suspicion that the juvenile may resist, attempt escape, injure him/herself, injure the officer, or damage property." Add to these limited circumstances that spit hoods may *only* be used where a person is already spitting or biting or reasonably believed to be about to do so, *and* that other restraints would generally be applied, it is difficult to imagine a scenario wherein a small child's behavior would somehow justify use of a spit hood.

The policy further provides substantial accountability, as section 302.13 requires officers to document within their report every instance wherein a spit hood is applied, and Body Worn Camera footage will support examination of any circumstance wherein a complaint of an inappropriate application is raised.

The Department's revised policy is attached in two versions, one showing markup, and one without markup.

Attachments:

July 5, 2019 revision of Policy 302, Handcuffing and Restraints, with no markup

July 5, 2019 revision of Policy 302, Handcuffing and Restraints, with markup

---

## Handcuffing and Restraints

### 302.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of handcuffs and other restraints during detentions and arrests.

### 302.2 POLICY

The Berkeley Police Department authorizes the use of restraint devices in accordance with this policy, the Use of Force policy and department training. Restraint devices shall not be used to punish, to display authority or as a show of force.

### 302.3 USE OF RESTRAINTS

Only members who have successfully completed Berkeley Police Department approved training on the use of restraint devices described in this policy are authorized to use these devices.

When deciding whether to use any restraint, officers should carefully balance officer safety concerns with factors that include, but are not limited to:

- (a) The circumstances or crime leading to the arrest
- (b) The demeanor and behavior of the arrested person
- (c) The age and health of the person
- (d) Whether the person may be pregnant
- (e) Whether the person has a hearing or speaking disability. In such cases, consideration should be given, safety permitting, to handcuffing to the front in order to allow the person to sign or write notes
- (f) Whether the person has any other apparent disability

### 302.4 RESTRAINT OF DETAINEES

Situations may arise where it may be reasonable to restrain an individual who may, after brief investigation, be released without arrest. Unless arrested, the use of restraints on detainees should continue only for as long as is reasonably necessary to assure the safety of officers and others. When deciding whether to remove restraints from a detainee, officers should continuously weigh the safety interests at hand against the continuing intrusion upon the detainee.

### 302.5 ALTERNATIVE MEANS OF RESTRAINT

Alternative Means of Restraint include but are not limited to:

- (a) Handcuffing the person with their hands in front of their body
- (b) Handcuffing the person with multiple sets of linked handcuffs
- (c) Use of the entire WRAP system

- 
- (d) Use of the WRAP's ankle strap
  - (e) Use of plastic handcuffs "flex-cuffs"
  - (f) An ambulance gurney with five point straps

### **302.6 RESTRAINT OF PREGNANT PERSONS**

Persons who are known to be pregnant should be restrained in the least restrictive manner that is effective for officer safety and in no event shall these persons be restrained by the use of leg irons, waist chains or handcuffs behind the body.

No person who is in labor, delivery or recovery after delivery shall be handcuffed or restrained except in extraordinary circumstances and only when a supervisor makes an individualized determination that such restraints are necessary for the safety of the arrestee, officers or others (Penal Code § 3407; Penal Code § 6030).

### **302.7 RESTRAINT OF JUVENILES**

A juvenile under 14 years of age should not be restrained unless he/she is suspected of a dangerous felony or when the officer has a reasonable suspicion that the juvenile may resist, attempt escape, injure him/herself, injure the officer or damage property.

### **302.8 NOTIFICATIONS**

Whenever an officer transports a person with the use of restraints other than handcuffs, the officer shall inform the jail staff upon arrival at the jail that restraints were used. This notification should include information regarding any other circumstances the officer reasonably believes would be potential safety concerns or medical risks to the subject (e.g., prolonged struggle, extreme agitation, impaired respiration) that may have occurred prior to, or during transportation to the jail.

### **302.9 APPLICATION OF HANDCUFFS OR PLASTIC CUFFS**

Handcuffs, including temporary plastic cuffs (aka "flex-cuffs"), may be used only to restrain a person's hands to ensure officer safety.

Although recommended for most arrest situations, handcuffing is not an absolute requirement of the Department. Officers should consider handcuffing any person they reasonably believe warrants that degree of restraint. However, officers should not conclude that regardless of the circumstances, every person should be handcuffed.

In most situations handcuffs should be applied with the hands behind the person's back. When feasible, handcuffs should be applied between the base of the palm and the ulna bone of the wrist. When feasible, handcuffs should be double-locked to prevent tightening, which may cause undue discomfort or injury to the hands or wrists.

In situations where one pair of handcuffs does not appear sufficient to restrain the individual or may cause unreasonable discomfort due to the person's size, officers should consider using alternative means of restraint.

If the person being handcuffed is on the ground or in a prone position, officers should, as soon as

---

possible, place the person in an upright sitting position or on their side for respiratory recovery and to mitigate the potential for positional asphyxia.

Handcuffs should be removed as soon as it is reasonable or after the person has been searched and is safely confined within a detention facility.

### **302.10 APPLICATION OF SPIT HOODS/MASKS/SOCKS**

Spit hoods, aka "spit masks" or "spit socks" are temporary protective devices designed to prevent the wearer from transferring or transmitting fluids (saliva and mucous) to others. As the Department recognizes that use of a spit hood may be experienced as a traumatic event to a wearer, and may cause alarm and concern to onlookers, this policy provides clear and specific guidelines for their use, in service of the safety of all parties involved.

Spit hoods may be placed upon persons in custody while the officer reasonably believes the person will bite or spit, either on a person or in an inappropriate place. They are generally used during application of a physical restraint, while the person is restrained, or during or after transport.

Officers utilizing spit hoods shall ensure that the spit hood is applied properly to allow for adequate ventilation and that the restrained person can breathe normally. Officers should provide assistance during the movement of restrained individuals due to the potential for impaired or distorted vision on the part of the individual. Officers should avoid comingling individuals wearing spit hoods with other detainees.

Spit hoods shall not be used in situations where there are indications that the restrained person has a medical condition evident in the area around the mouth or nose, such as difficulty breathing or vomiting. In such cases, prompt medical care should be provided. If the person vomits while wearing a spit hood, the spit hood shall be promptly removed and discarded. Persons who have been sprayed with oleoresin capsicum (OC) spray should be thoroughly decontaminated including hair, head and clothing prior to application of a spit hood.

Those who have been placed in a spit hood should be continually monitored and shall not be left unattended until the spit hood is removed. Spit hoods shall be discarded after each use.

### **302.11 APPLICATION OF THE WRAP**

The WRAP is a temporary restraining device comprised of a Velcro strapped leg panel, torso harness, ankle strap and backside handcuff carabiner. The device immobilizes the body into a straight-legged seated position. Used properly, it restricts a subject's ability to do harm to oneself or others. Officer safety is enhanced and the risk of injury to the subject is reduced.

In determining whether to use the WRAP, officers should consider:

- (a) Whether the officer or others could be exposed to injury due to the assaultive or resistant behavior of a suspect.
- (b) Whether it is reasonably necessary to protect the suspect from his/her own actions (e.g., running away from the arresting officer while handcuffed, kicking at objects or officers).



- 
- (c) Whether it is reasonably necessary to avoid damage to property (e.g., kicking at windows of the patrol unit).
  - (d) Whether conventional methods of restraint have failed.

#### 302.11.1 GUIDELINES FOR USE OF THE WRAP

When applying the WRAP the following guidelines should be followed:

- (a) If practicable, officers should notify a supervisor of the intent to apply the WRAP. In all cases, a supervisor shall be notified as soon as practicable after the application of the WRAP.
- (b) Once applied, absent a medical or other emergency, restraints should remain in place until the officer arrives at the jail or other facility or the person no longer reasonably appears to pose a threat.
- (c) Restraint straps should be checked frequently for tightness, and adjusted as necessary until the WRAP is removed. The harness straps shall never be tightened to the point they interfere with the person's ability to breathe.
- (d) The restrained person should be continually monitored by an officer while the WRAP is in use. The officer should ensure that the person does not roll onto and remain on his/her stomach.
- (e) The officer should look for signs of distress such as sudden quiet or inactivity, complaints of chest pain, change in facial color, complaint of extreme heat, vomiting and/or labored breathing, and take appropriate steps to relieve and minimize any obvious factors contributing to this condition.
- (f) Movement of the person can be accomplished in three ways, depending on the level of their cooperation. The person can either be carried, allowed to stand and shuffle walk, or be transported in a vehicle.
- (g) Once secured in a vehicle, the person should be placed in a seated or upright position, secured with a seat belt, and shall not be placed on his/her stomach for an extended period, as this could reduce the person's ability to breathe.
- (h) If in custody and transported by ambulance/paramedic unit, the restrained person should be accompanied by an officer when requested by medical personnel. The transporting officer should describe to medical personnel any unusual behaviors or other circumstances the officer reasonably believes would be potential safety or medical risks to the subject (e.g., prolonged struggle, extreme agitation, impaired respiration).

#### 302.11.2 DEVICE REMOVAL

Based on the person's combativeness or level of aggression, officers should employ appropriate control techniques and tactics when removing the WRAP.

---

### 302.11.3 THE WRAP'S ANKLE STRAP

The ankle strap is a part of the WRAP restraint system. The ankle strap may be used alone, without the rest of the WRAP system to restrain the legs of a violent or potentially violent person when it is reasonable to do so during the course of detention, arrest or transportation. Use of the ankle strap will follow the same guidelines listed above for the WRAP.

### 302.12 APPLICATION OF AUXILIARY RESTRAINT DEVICES

Auxiliary restraint devices include transport belts, waist or belly chains, transportation chains, leg irons and other similar devices. Auxiliary restraint devices are intended for use during long-term restraint or transportation. They provide additional security and safety without impeding breathing, while permitting adequate movement, comfort and mobility.

Only department-authorized devices may be used. Any person in auxiliary restraints should be monitored as reasonably appears necessary.

### 302.13 REQUIRED DOCUMENTATION

If an individual is restrained and released without an arrest, the officer shall document the details of the detention and the need for handcuffs or other restraints.

If an individual is arrested, the use of restraints other than handcuffs shall be documented in the related report. The officer should include, as appropriate:

- (a) How the suspect was transported and the position of the suspect.
- (b) Observations of the suspect's behavior and any signs of physiological problems.
- (c) Any known or suspected drug use or other medical problems.

## Handcuffing and Restraints

### 302.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of handcuffs and other restraints during detentions and arrests.

### 302.2 POLICY

The Berkeley Police Department authorizes the use of restraint devices in accordance with this policy, the Use of Force policy and department training. Restraint devices shall not be used to punish, to display authority or as a show of force.

### 302.3 USE OF RESTRAINTS

Only members who have successfully completed Berkeley Police Department approved training on the use of restraint devices described in this policy are authorized to use these devices.

When deciding whether to use any restraint, officers should carefully balance officer safety concerns with factors that include, but are not limited to:

- (a) The circumstances or crime leading to the arrest
- (b) The demeanor and behavior of the arrested person
- (c) The age and health of the person
- (d) Whether the person may be known to be pregnant
- (e) Whether the person has a hearing or speaking disability. In such cases, consideration should be given, safety permitting, to handcuffing to the front in order to allow the person to sign or write notes
- (f) Whether the person has any other apparent disability

### 302.4 RESTRAINT OF DETAINEES

Situations may arise where it may be reasonable to restrain an individual who may, after brief investigation, be released without arrest. Unless arrested, the use of restraints on detainees should continue only for as long as is reasonably necessary to assure the safety of officers and others. When deciding whether to remove restraints from a detainee, officers should continuously weigh the safety interests at hand against the continuing intrusion upon the detainee.

### 302.5 ALTERNATIVE MEANS OF RESTRAINT

Alternative Means of Restraint include but are not limited to:

- (a) Handcuffing the person with their hands in front of their body
- (b) Handcuffing the person with multiple sets of linked handcuffs

- (c) Use of the entire WRAP system
- (d) Use of the WRAP's ankle strap
- (e) Use of plastic handcuffs "flex-cuffs"
- (f) An ambulance gurney with five point straps

#### 302.5302.6 RESTRAINT OF PREGNANT PERSONS

Persons who are known to be pregnant should be restrained in the least restrictive manner that is effective for officer safety and in no event shall these persons be restrained by the use of leg irons, waist chains or handcuffs behind the body.

No person who is in labor, delivery or recovery after delivery shall be handcuffed or restrained except in extraordinary circumstances and only when a supervisor makes an individualized determination that such restraints are necessary for the safety of the arrestee, officers or others (Penal Code § 3407; Penal Code § 6030).

#### 302.6302.7 RESTRAINT OF JUVENILES

A juvenile under 14 years of age should not be restrained unless he/she is suspected of a dangerous felony or when the officer has a reasonable suspicion that the juvenile may resist, attempt escape, injure him/herself, injure the officer or damage property.

#### 302.7302.8 NOTIFICATIONS

Whenever an officer transports a person with the use of restraints other than handcuffs, the officer shall inform the jail staff upon arrival at the jail that restraints were used. This notification should include information regarding any other circumstances the officer reasonably believes would be potential safety concerns or medical risks to the subject (e.g., prolonged struggle, extreme agitation, impaired respiration) that may have occurred prior to, or during transportation to the jail.

#### 302.8302.9 APPLICATION OF HANDCUFFS OR PLASTIC CUFFS

Handcuffs, including temporary ~~nylon or~~ plastic cuffs (aka "flex-cuffs"), may be used only to restrain a person's hands to ensure officer safety.

Although recommended for most arrest situations, handcuffing is ~~discretionary and~~ not an absolute requirement of the Department. Officers should consider handcuffing any person they reasonably believe warrants that degree of restraint. However, officers should not conclude that regardless of the circumstances, in order to avoid risk every person should be handcuffed. ~~regardless of the circumstances~~

In most situations handcuffs should be applied with the hands behind the person's back. When feasible, handcuffs should be applied between the base of the palm and the ulna bone of the wrist. When feasible, handcuffs should be double-locked to prevent tightening, which may cause undue discomfort or injury to the hands or wrists.

In situations where one pair of handcuffs does not appear sufficient to restrain the individual or may cause unreasonable discomfort due to the person's size, officers should consider using alternative

Commented [SSM1]: Jun 2019 - Section changed back to Lexipol language from our prior H6 language - per the PRC 6/18/19

~~means of restraint alternatives, such as using an additional set of handcuffs or multiple plastic cuffs~~

~~If the person being handcuffed is on the ground or in a prone position, officers should, as soon as possible, place the person in an upright sitting position or on their side for respiratory recovery and to mitigate the potential for positional asphyxia.~~

Commented [SSM2]: Sep 2018 - Added per PRC request from 9/17/18

Handcuffs should be removed as soon as it is reasonable or after the person has been searched and is safely confined within a detention facility.

### 302.9302.10 APPLICATION OF SPIT HOODS/MASKS/SOCKS

Spit hoods, ~~aka "spit masks" or "spit socks"/masks/socks~~ are temporary protective devices designed to prevent the wearer from ~~biting and/or~~ transferring or transmitting fluids (saliva and mucous) to others. ~~As the Department recognizes that use of a spit hood may be experienced as a traumatic event to a wearer, and may cause alarm and concern to onlookers, this policy provides clear and specific guidelines for their use, in service of the safety of all parties involved.~~

Commented [SSM3]: Jun 2019 - Changed back to "hoods" per PRC 6/18/19 meeting

Commented [SSM4]: Jun 2019 - Chief's language

Commented [GA5]: July 5 language added re: traumatic to the wearer

Spit hoods may be placed upon persons in custody ~~when~~ while the officer reasonably believes the person will bite or spit, either on a person or in an inappropriate place. They are generally used during application of a physical restraint, while the person is restrained, or during or after transport.

Commented [GA6]: July 5 language added, using "while" instead of "when", based on PRC input

Officers utilizing spit hoods ~~shall~~ should ensure that the spit hood is ~~applied~~ fastened properly to allow for adequate ventilation and that the restrained person can breathe normally. Officers should provide assistance during the movement of restrained individuals due to the potential for impaired or distorted vision on the part of the individual. Officers should avoid comingling individuals wearing spit hoods with other detainees.

Commented [SSM7]: Jun 2019 - Shall per PRC 6/18/19 meeting

Spit hoods ~~shall~~ should not be used in situations where ~~the restrained person is bleeding profusely from the area around the mouth or nose, or if~~ there are indications that the ~~restrained~~ person has a medical condition ~~evident in the area around the mouth or nose~~, such as difficulty breathing or vomiting. In such cases, prompt medical care should be ~~provided~~ obtained. If the person vomits while wearing a spit hood, the spit hood ~~shall~~ should be promptly removed and discarded. Persons who have been sprayed with oleoresin capsicum (OC) spray should be thoroughly decontaminated including hair, head and clothing prior to application of a spit hood.

Commented [SSM8]: Jun 21 - changed back to shall - accidental deletion in previous version.

Commented [SSM9]: Jun 12 2019 Chief's changes

Those who have been placed in a spit hood should be continually monitored and shall not be left unattended until the spit hood is removed. Spit hoods shall be discarded after each use.

Commented [SSM10]: Jun 2019 - Per PRC

### 302.10302.11 APPLICATION OF THE WRAPLEG RESTRAINT DEVICES

The WRAP is a temporary restraining device comprised of a Velcro strapped leg panel, torso harness, ankle strap and backside handcuff carabiner. The device immobilizes the body into a straight-legged seated position. Used properly, it restricts a subject's ability to do harm to oneself or others. Officer safety is enhanced and the risk of injury to the subject is reduced.

~~Leg restraints may be used to restrain the legs of a violent or potentially violent person when it is reasonable to do so during the course of detention, arrest or transportation. Only restraint devices approved by the Department shall be used.~~

In determining whether to use the WRAP leg restraint, officers should consider:

- (a) Whether the officer or others could be exposed to injury due to the assaultive or resistant behavior of a suspect.
- (b) Whether it is reasonably necessary to protect the suspect from his/her own actions (e.g., ~~hitting his/her head against the interior of the patrol unit,~~ running away from the arresting officer while handcuffed, kicking at objects or officers).
- (c) Whether it is reasonably necessary to avoid damage to property (e.g., kicking at windows of the patrol unit).
- (d) Whether conventional methods of restraint have failed.

#### 302.11.1 GUIDELINES FOR USE OF THE WRAP LEG RESTRAINTS

When applying the WRAP leg restraints the following guidelines should be followed:

- (a) If practicable, officers should notify a supervisor of the intent to apply the ankle-WRAP strap device. In all cases, a supervisor shall be notified as soon as practicable after the application of the ankle strap device WRAP.
- (b) Once applied, absent a medical or other emergency, restraints should remain in place until the officer arrives at the jail or other facility or the person no longer reasonably appears to pose a threat.
- (c) Restraint straps should be checked frequently for tightness, and adjusted as necessary until the WRAP is removed. The harness straps shall never be tightened to the point they interfere with the person's ability to breathe.
- (d) The restrained person should be continually monitored by an officer while the WRAP ankle strap is in use. The officer should ensure that the person does not roll onto and remain on his/her stomach.
- (e) The officer should look for signs of distress such as sudden quiet or inactivity, complaints of chest pain, change in facial color, complaint of extreme heat, vomiting and/or labored breathing, and take appropriate steps to relieve and minimize any obvious factors contributing to this condition.
- (f) Movement of the person can be accomplished in three ways, depending on the level of their cooperation. The person can either be carried, allowed to stand and shuffle walk, or be transported in a vehicle.
- (g) Once secured in a vehicle, the person should be placed in a seated or upright position,

Commented [SSM11]: Per PRC 6/18/19

Commented [SSM12]: Per PRC 6/18/19

---

secured with a seat belt, and shall not be placed on his/her stomach for an extended period, as this could reduce the person's ability to breathe.

- (h) If in custody and transported by ambulance/paramedic unit, the restrained person should be accompanied by an officer when requested by medical personnel. The transporting officer should describe to medical personnel any unusual behaviors or other circumstances the officer reasonably believes would be potential safety or medical risks to the subject (e.g., prolonged struggle, extreme agitation, impaired respiration).

### 302.11.2 DEVICE REMOVAL

Based on the person's combativeness or level of aggression, officers should employ appropriate control techniques and tactics when removing the WRAP.

### 302.11.3 THE WRAP'S ANKLE STRAP

The ankle strap is a part of the WRAP restraint system. The ankle strap may be used alone, without the rest of the WRAP system to restrain the legs of a violent or potentially violent person when it is reasonable to do so during the course of detention, arrest or transportation. Use of the ankle strap will follow the same guidelines listed above for the WRAP.

### 302.11302.12 APPLICATION OF AUXILIARY RESTRAINT DEVICES

Auxiliary restraint devices include transport belts, waist or belly chains, transportation chains, leg irons and other similar devices. Auxiliary restraint devices are intended for use during long-term restraint or transportation. They provide additional security and safety without impeding breathing, while permitting adequate movement, comfort and mobility.

Only department-authorized devices may be used. Any person in auxiliary restraints should be monitored as reasonably appears necessary.

### 302.12302.13 REQUIRED DOCUMENTATION

If an individual is restrained and released without an arrest, the officer shall document the details of the detention and the need for handcuffs or other restraints.

If an individual is arrested, the use of restraints other than handcuffs shall be documented in the related report. The officer should include, as appropriate:

~~(a) — The amount of time the suspect was restrained.~~

~~(b)(a).~~ How the suspect was transported and the position of the suspect.

~~(c)(b).~~ Observations of the suspect's behavior and any signs of physiological problems.

~~(d)(c).~~ Any known or suspected drug use or other medical problems.

1

2

3



Lee, Katherine

---

**From:** J. George Lippman <george@igc.org>  
**Sent:** Tuesday, July 09, 2019 8:46 PM  
**To:** All Council: Igor Tregub; George Perezvelez; Lee, Katherine; Kitty Calavita; Manager, C; Greenwood, Andrew  
**Subject:** Fwd: Dajuan Armstrong suffocated from spit mask and restraints

FYI

Begin forwarded message:

**From:** Rivka Polatnick <rivkapol@hotmail.com>  
**Subject:** Dajuan Armstrong suffocated from spit mask and restraints  
**Date:** July 9, 2019 at 8:37:05 PM PDT  
**To:** George Lippman <george@igc.org>, Marc Staton <marcsville@gmail.com>, Andrea Prichett <prichett@locrian.com>

The D.A.'s report on Dajuan Armstrong's death a year ago in Santa Rita has just been released, and the East Bay Express is reporting:

"Alameda County Sheriff's deputies used a full-body restraint device and a spit mask on an inmate they were escorting to the outpatient housing unit in Santa Rita Jail last year, which caused his death by asphyxiation, according to a report by the Alameda County District Attorney's Office clearing the deputies of criminal charges."

See the article:

<https://www.eastbayexpress.com/oakland/santa-rita-inmate-suffocated-from-restraints-used-by-deputies/Content?oid=26891586>



# SURVEILLANCE - PUBLIC COPY

## Surveillance Technology Use & Community Safety Ordinance -- Guide to documents distributed to the PRC

The Ordinance was included in the PRC's May 22, 2019 packet, and the remaining documents were distributed to the PRC at that meeting. The underlined documents have been revised and are included in the agenda packet for the July 10, 2019 meeting.

### ORDINANCE

Berkeley Municipal Code Ch. 2.99 – Acquisition and Use of Surveillance Technology

### BODY WORN CAMERAS (BWCs)

Policy 1300 Surveillance Use Policy

Policy 1300 Appendix A – Surveillance Acquisition Report

Policy 425 Body Worn Cameras (issued 9-28-18, rev. 1-31-19)

### GLOBAL POSITIONING SYSTEM (GPS) TRACKING DEVICES

Policy 1301 Surveillance Use Policy

Policy 1301 Appendix A – Surveillance Acquisition Report

### AUTOMATED LICENSE PLATE READERS (ALPRs)

Policy 1302 Surveillance Use Policy

Policy 1302 Appendix A – Surveillance Acquisition Report

Policy 422 ALPRs (proposed conversion of Admin. Order to Lexipol)

Administrative Order #001-2016 ALPRs (issued 2-18-16)

ZUR VERLEIHUNG VON FACHLICHEM RANG

## Chapter 2.99

### ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

#### Sections:

<b>2.99.010</b>	<b>Purposes</b>
<b>2.99.020</b>	<b>Definitions</b>
<b>2.99.030</b>	<b>City Council Approval Requirement</b>
<b>2.99.040</b>	<b>Temporary Acquisition and Use of Surveillance Equipment</b>
<b>2.99.050</b>	<b>Compliance for Existing Surveillance Technology</b>
<b>2.99.060</b>	<b>Determination by City Council that Benefits Outweigh Costs and Concerns</b>
<b>2.99.070</b>	<b>Oversight Following City Council Approval</b>
<b>2.99.080</b>	<b>Public Access to Surveillance Technology Contracts</b>
<b>2.99.090</b>	<b>Enforcement</b>
<b>2.99.100</b>	<b>Whistleblower Protections</b>
<b>2.99.110</b>	<b>Severability</b>

#### **2.99.010 Purposes**

A. Through the enactment of this Chapter, the City seeks to establish a thoughtful process regarding the procurement and use of Surveillance Technology that carefully balances the City's interest in protecting public safety with its interest in protecting the privacy and civil rights of its community members.

B. Transparency is essential when the City is considering procurement and use of Surveillance Technology.

C. Although such technology may be beneficial to public order and safety, it has the potential to put both privacy and civil liberties at risk.

D. Decisions relating to Surveillance Technology should occur with strong consideration of the impact such technologies may have on civil rights and civil liberties, as with all rights guaranteed by the California and United States Constitutions.

E. Surveillance Technology may involve immediate, as well as ongoing, financial costs. Before the City acquires any Surveillance Technology, it must evaluate all costs associated with the procurement, installation, use and maintenance of the technology.

F. Decisions regarding whether and how Surveillance Technologies should be funded, acquired, or used should be governed by the City Council as the elected representatives of the City.

G. In addition to applicable local, state, and federal law, legally enforceable safeguards, including robust transparency, oversight, and accountability measures, are important in the protection of civil rights and civil liberties.

H. Data reporting measures will enable the City Council and public to confirm that mandated civil rights and civil liberties safeguards have been strictly observed. (Ord. 7592-NS § 2 (part), 2018)

### **2.99.020 Definitions**

The following definitions apply to this Chapter:

1. "Surveillance Technology" means an electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of covered Surveillance Technology include, but are not limited to: cell site simulators (Stingrays); automatic license plate readers; body worn cameras; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems, except as allowed under Section 1(d); social media analytics software; gait analysis software; and video cameras that record audio or video and can remotely transmit or can be remotely accessed.

"Surveillance Technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a Surveillance Technology as defined in Section 1 (above):

- a. Routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance functions;
- b. Handheld Parking Citation Devices, that do not automatically read license plates;
- c. Manually-operated, portable digital cameras, audio recorders, and video recorders that are not to be used remotely and whose functionality is limited to manually capturing, viewing, editing and downloading video and/or audio recordings, but not including body worn cameras;
- d. Devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles or thermal imaging cameras used for fire operations, search and rescue operations and missing person searches, and equipment used in active searches for wanted suspects;
- e. Manually-operated technological devices that are not designed and will not be used to surreptitiously collect surveillance data, such as two-way radios, email systems and city-issued cell phones;
- f. Municipal agency databases;
- g. Medical equipment used to diagnose, treat, or prevent disease or injury, including electrocardiogram machines;

h. Cybersecurity capabilities, technologies and systems used by the City of Berkeley Department of Information Technology to predict, monitor for, prevent, and protect technology infrastructure and systems owned and operated by the City of Berkeley from potential cybersecurity events and cyber-forensic based investigations and prosecutions of illegal computer based activity;

i. Stationary security cameras affixed to City property or facilities.

2. "Surveillance Technology Report" means an annual written report by the City Manager covering all of the City of Berkeley's Surveillance Technologies that includes all of the following information with regard to each type of Surveillance Technology:

a. 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;

b. Geographic Deployment: Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically;

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

d. 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;

e. 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;

f. Effectiveness: Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes;

g. Costs: Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.

3. "Surveillance Acquisition Report" means a publicly-released written report produced prior to acquisition or to proposed permanent use after use in Exigent Circumstances pursuant to Section 2.99.040 (2), of a type of Surveillance Technology that includes the following:

a. Description: Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers;

- b. Purpose: Information on the proposed purpose(s) for the Surveillance Technology;
  - c. Location: The general location(s) it may be deployed and reasons for deployment;
  - d. Impact: An assessment identifying potential impacts on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups;
  - e. Mitigation: Information regarding technical and procedural measures that can be implemented to appropriately safeguard the public from any impacts identified in subsection (d);
  - f. Data Types and Sources: A list of the sources of data proposed to be collected, analyzed, or processed by the Surveillance Technology, including "open source" data;
  - g. Data Security: Information about the steps that can be taken to ensure adequate security measures to safeguard the data collected or generated from unauthorized access or disclosure;
  - h. Fiscal Cost: The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, including to the extent practicable costs associated with compliance with this and other reporting and oversight requirements, as well as any current or potential sources of funding;
  - i. Third Party Dependence and Access: Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis, and whether a third party may have access to such data or may have the right to sell or otherwise share the data in aggregated, disaggregated, raw or any other formats;
  - j. Alternatives: A summary and general assessment of potentially viable alternative methods (whether involving the use of a new technology or not), if any, considered before deciding to propose acquiring the Surveillance Technology; and
  - k. Experience of Other Entities: To the extent such information is available, a summary of the experience of comparable government entities with the proposed technology, including any unanticipated financial or community costs and benefits, experienced by such other entities.
4. "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of each type of the Surveillance Technology that shall reflect the Surveillance Acquisition Report produced for that Surveillance Technology and that at a minimum specifies the following:
- a. Purpose: The specific purpose(s) that the Surveillance Technology is intended to advance;



- b. **Authorized Use:** The uses that are authorized, the rules and processes required prior to such use, and the uses that are prohibited;
  - c. **Data Collection:** Information collection that is allowed and prohibited. Where applicable, list any data sources the technology will rely upon, including "open source" data;
  - d. **Data Access:** A general description of the title and position of the employees and entities authorized to access or use the collected information, and the rules and processes required prior to access or use of the information, and a description of any and all of the vendor's rights to access and use, sell or otherwise share information for any purpose;
  - e. **Data Protection:** A general description of the safeguards that protect information from unauthorized access, including encryption and access control mechanisms, and safeguards that exist to protect data at the vendor level;
  - f. **Civil Liberties and Rights Protection:** A general description of the safeguards that protect against the use of the Surveillance Technology and any data resulting from its use in a way that violates or infringes on civil rights and liberties, including but not limited to potential disparate or adverse impacts on any communities or groups;
  - g. **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond such period;
  - h. **Public Access:** How collected information may be accessed or used by members of the public;
  - i. **Third Party Data Sharing:** If and how other City or non-City Entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
  - j. **Training:** Training required for any employee authorized to use the Surveillance Technology or to access information collected;
  - k. **Auditing and Oversight:** Mechanisms to ensure that the Surveillance Use Policy is followed, technical measures to monitor for misuse, and the legally enforceable sanctions for intentional violations of the policy; and
  - l. **Maintenance:** The mechanisms and procedures to ensure maintenance of the security and integrity of the Surveillance Technology and collected information.
5. "Exigent Circumstances" means the City Manager's good faith belief that an emergency involving imminent danger of death or serious physical injury to any

person, or imminent danger of significant property damage, requires use of the Surveillance Technology or the information it provides. (Ord. 7592-NS § 2 (part), 2018)

### **2.99.030 City Council Approval Requirement**

1. The City Manager must obtain City Council approval, except in Exigent Circumstances, by placing an item on the Action Calendar at a duly noticed meeting of the City Council prior to any of the following:

- a. Seeking, soliciting, or accepting grant funds for the purchase of, or in-kind or other donations of, Surveillance Technology;
- b. Acquiring new Surveillance Technology, including but not limited to procuring such technology without the exchange of monies or consideration;
- c. Using new Surveillance Technology, or using Surveillance Technology previously approved by the City Council for a purpose, or in a manner not previously approved by the City Council; or
- d. Entering into an agreement with a non-City entity to acquire, share or otherwise use Surveillance Technology or the information it provides, or expanding a vendor's permission to share or otherwise use Surveillance Technology or the information it provides.

2. The City Manager must present a Surveillance Use Policy for each Surveillance Technology to the Police Review Commission, prior to adoption by the City Council. The Police Review Commission shall also be provided with the corresponding Surveillance Acquisition Report that had been presented to council for that Surveillance Technology. No later than 30 days after receiving a Surveillance Use Policy for review, the Police Review Commission must vote to recommend approval of the policy, object to the proposal, recommend modifications, or take no action. Neither opposition to approval of such a policy, nor failure by the Police Review Commission to act, shall prohibit the City Manager from proceeding with its own review and potential adoption.

3. The City Manager must submit for review a Surveillance Acquisition Report and obtain City Council approval of a Surveillance Use Policy prior to engaging in any of the activities described in subsections (1) (a)-(d). (Ord. 7592-NS § 2 (part), 2018)

### **2.99.040 Temporary Acquisition and Use of Surveillance Equipment**

Notwithstanding the provisions of this Chapter, the City Manager may borrow, acquire and/or temporarily use Surveillance Technology in Exigent Circumstances without following the requirements in Sections 2.99.030 and 2.99.040. However, if the City Manager borrows, acquires or temporarily uses Surveillance Technology in Exigent Circumstances he or she must take all of the following actions:

1. Provide written notice of that acquisition or use to the City Council within 30 days following the commencement of such Exigent Circumstance, unless such information is confidential or privileged;

2. If it is anticipated that the use will continue beyond the Exigent Circumstance, submit a proposed Surveillance Acquisition Report and Surveillance Use Policy, as applicable, to the City Council within 90 days following the borrowing, acquisition or temporary use, and receive approval, as applicable, from the City Council pursuant to Sections 2.99.030 and 2.99.040; and

3. Include the Surveillance Technology in the City Manager's next annual Surveillance Technology Report. (Ord. 7592-NS § 2 (part), 2018)

#### **2.99.050 Compliance for Existing Surveillance Technology**

The City Manager shall submit to the Action Calendar for the first City Council meeting in November of 2018 a Surveillance Acquisition Report and a proposed Surveillance Use Policy for each Surveillance Technology possessed or used prior to the effective date of the ordinance codified in this Chapter. (Ord. 7592-NS § 2 (part), 2018)

#### **2.99.060 Determination by City Council that Benefits Outweigh Costs and Concerns**

The City Council shall only approve any action described in Section 2.99.030, 2.99.040, or Section 2.99.050 of this Chapter after making a determination that the benefits to the community of the Surveillance Technology, used according to its Surveillance Use Policy, outweigh the costs; that the proposal will appropriately safeguard civil liberties and civil rights to the maximum extent possible while serving its intended purposes; and that, in the City Council's judgment, no feasible alternative with similar utility and a lesser impact on civil rights or civil liberties could be implemented. (Ord. 7592-NS § 2 (part), 2018)

#### **2.99.070 Oversight Following City Council Approval**

The City Manager must submit to the Council Action Calendar a written Surveillance Technology Report, covering all of the City's Surveillance Technologies, annually at the first regular Council meeting in November. After review of the Surveillance Technology Report, Council may make modifications to Surveillance Use Policies. (Ord. 7592-NS § 2 (part), 2018)

#### **2.99.080 Public Access to Surveillance Technology Contracts**

To the extent permitted by law, the City shall continue to make available to the public all of its surveillance-related contracts, including related non-disclosure agreements, if any. (Ord. 7592-NS § 2 (part), 2018)

### **2.99.090 Enforcement**

This Chapter does not confer any rights upon any person or entity other than the City Council to cancel or suspend a contract for a Surveillance Technology. The Chapter does not provide a private right of action upon any person or entity to seek injunctive relief against the City or any employee unless that person or entity has first provided written notice to the City Manager by serving the City Clerk, regarding the specific alleged violations of this Chapter. If a specific alleged violation is not remedied within 90 days of that written notice, a person or entity may seek injunctive relief in a court of competent jurisdiction. If the alleged violation is substantiated and subsequently cured, a notice shall be posted in a conspicuous manner on the City's website that describes, to the extent permissible by law, the corrective measures taken to address the violation. If it is shown that the violation is the result of arbitrary or capricious action by the City or an employee or agent thereof in his or her official capacity, the prevailing complainant in an action for relief may collect from the City reasonable attorney's fees in an amount not to exceed \$15,000 if he or she is personally obligated to pay such fees. (Ord. 7592-NS § 2 (part), 2018)

### **2.99.100 Whistleblower Protections**

All provisions of Berkeley's Protection of Whistleblowers Workplace Policy, as promulgated by the City Manager on November 2, 2016 and including any updates or replacements thereto, shall apply. (Ord. 7592-NS § 2 (part), 2018)

### **2.99.110 Severability**

If any word, phrase, sentence, part, section, subsection, or other portion of this Chapter, or any application thereof to any person or circumstance, is declared void, unconstitutional, or invalid for any reason, then such word, phrase, sentence, part, section, subsection, or other portion, or the prescribed application thereof, shall be severable, and the remaining provisions of this Chapter, and all applications thereof, not having been declared void, unconstitutional or invalid, shall remain in full force and effect. The City Council hereby declares that it would have passed this title, and each section, subsection, sentence, clause and phrase of this Chapter, irrespective of the fact that any one or more sections, subsections, sentences, clauses or phrases is declared invalid or unconstitutional. (Ord. 7592-NS § 2 (part), 2018)

## Surveillance Use Policy - Body Worn Cameras

### 1300.1 PURPOSE

This Surveillance Use Policy is issued in compliance with BMC 2.99, and incorporates 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 officer(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

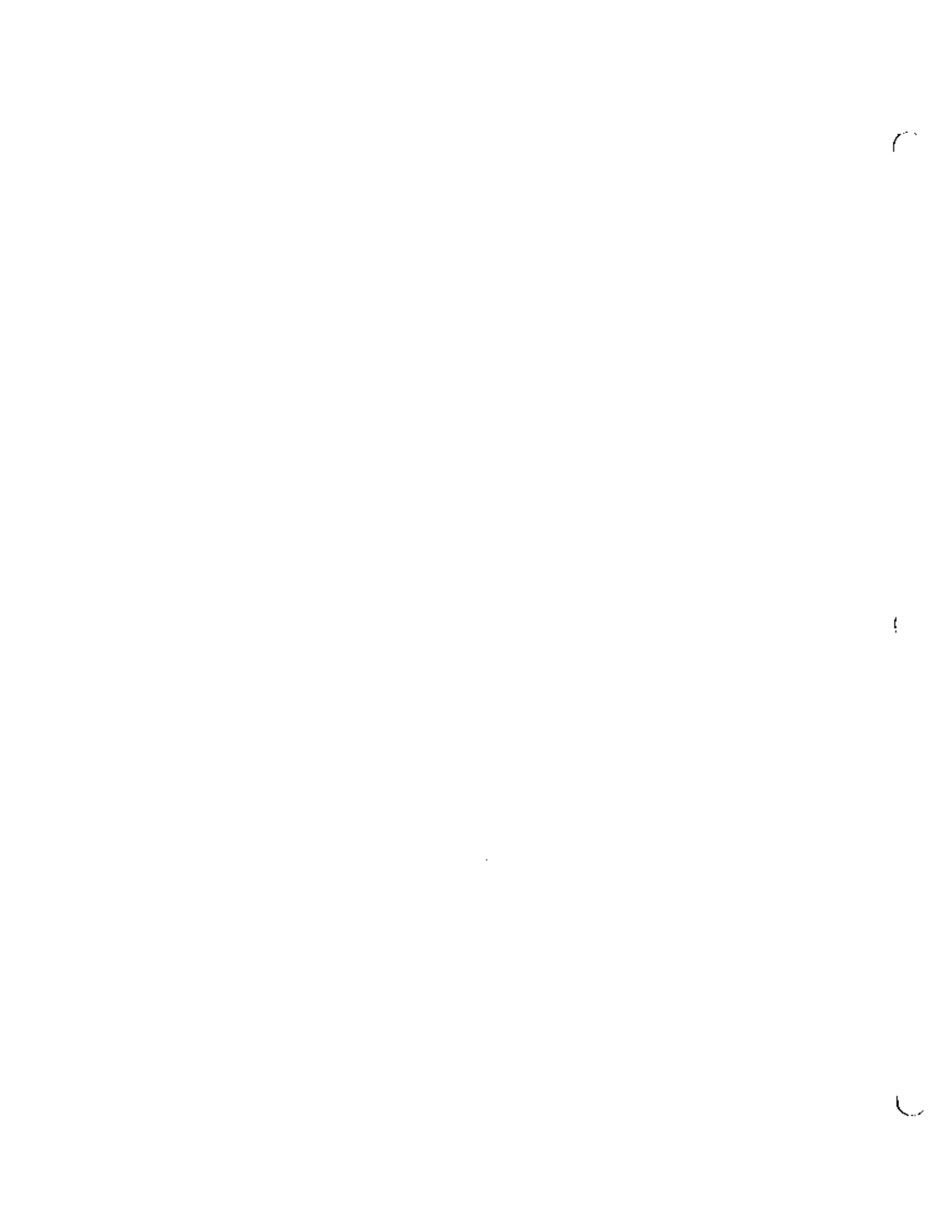
Division Captains for divisions utilizing BWC's shall ensure compliance with this Surveillance Use Policy.

### 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 cannot 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:

3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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 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"

#### **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 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.

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.

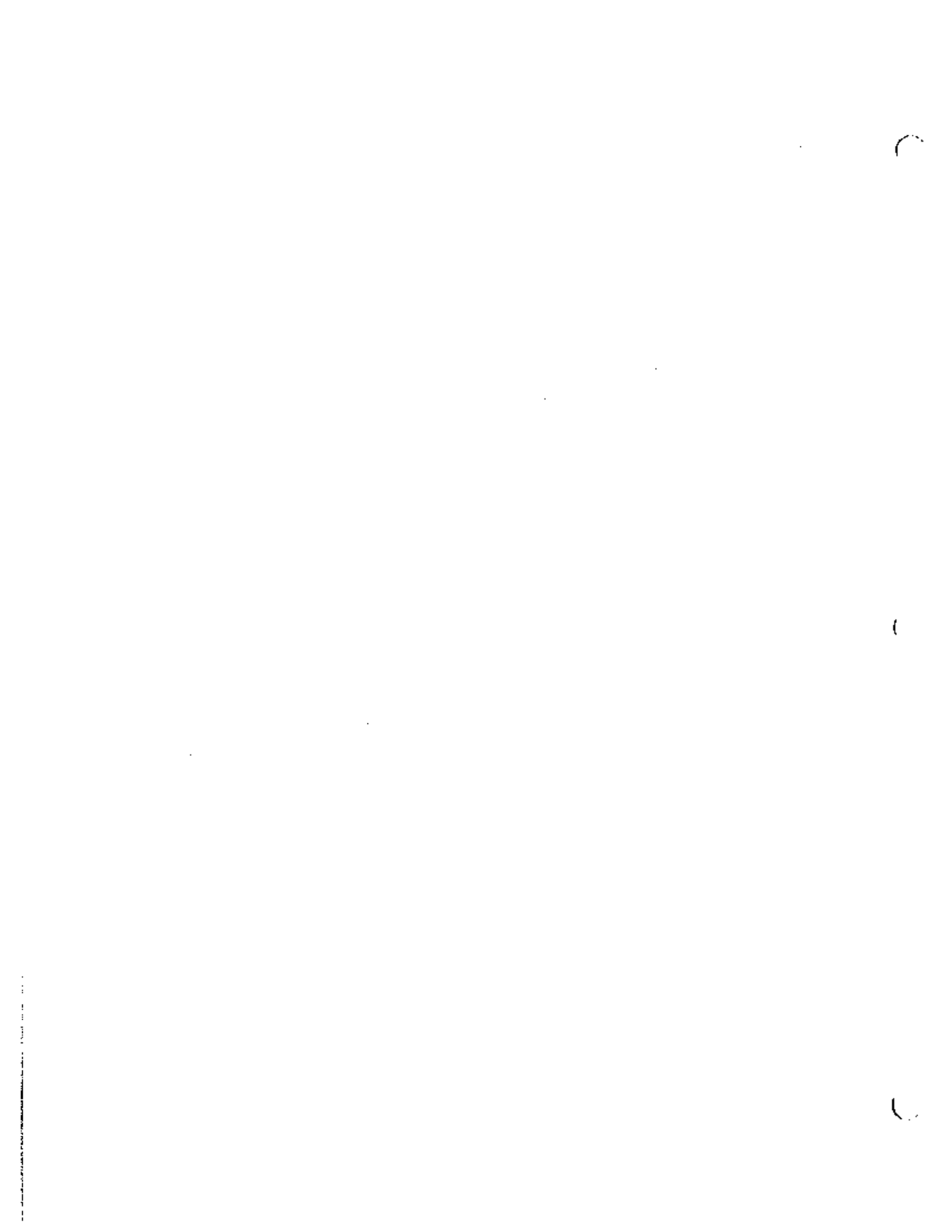
BWC technology provides video and audio documentation of policing activity in addition to the oral and written statements of officers, victims, and witnesses. Alternatives to the use of BWCs would be vehicle-based cameras and/or not utilizing BWCs. However, BPD sees the use of BWCs as an integral strategy 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](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.bwcorecard.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.

**Berkeley Police Department**  
Law Enforcement Services Manual

*Body Worn Cameras*

---

- (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

# Berkeley Police Department

## Law Enforcement Services Manual

### Body Worn Cameras

---

(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.

**Berkeley Police Department**  
Law Enforcement Services Manual

*Body Worn Cameras*

---

**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.



### *Body Worn Cameras*

---

#### **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.

# Berkeley Police Department

## Law Enforcement Services Manual

### Body Worn Cameras

---

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.

## *Body Worn Cameras*

---

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

**Berkeley Police Department**  
Law Enforcement Services Manual

Body Worn Cameras

---

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.

# Berkeley Police Department

## Law Enforcement Services Manual

### *Body Worn Cameras*

---

#### **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).

# Berkeley Police Department

## Law Enforcement Services Manual

### Body Worn Cameras

---

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."

# Berkeley Police Department

Law Enforcement Services Manual

## *Body Worn Cameras*

---

### **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**

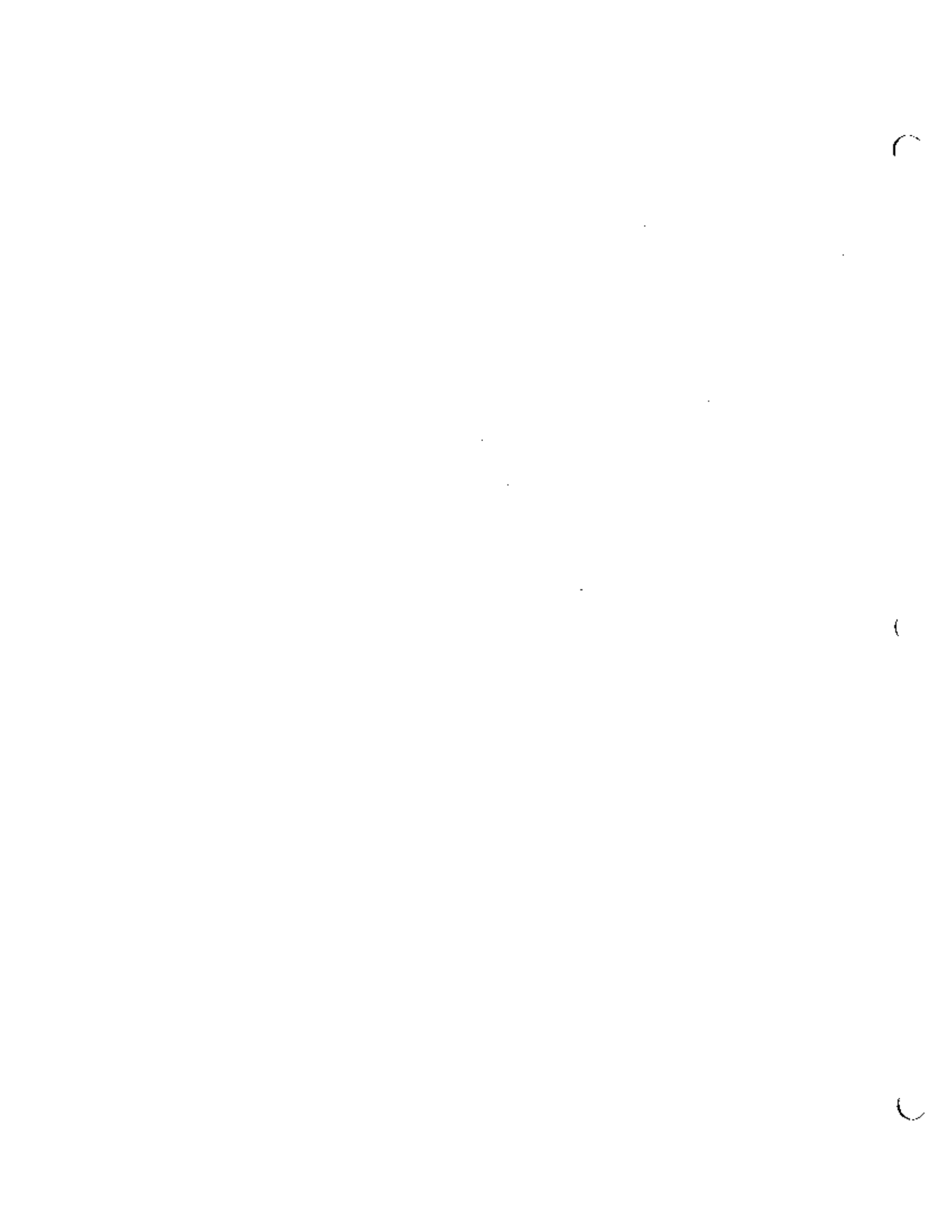
This policy shall comply at all times with the requirement of BMC 2.99 Acquisition and Use of Surveillance Technology.

### **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.





## Surveillance Use Policy - GPS Tracking Devices

### 1301.1 PURPOSE

Global Positioning System (GPS) tracking devices designed to track the movements of vehicles, bicycles, cargo, machinery, and other items. GPS trackers are utilized during active criminal investigations and shall be used pursuant to a lawfully issued search warrant, court order or with consent.

### 1301.2 AUTHORIZED USE

GPS trackers shall only be used pursuant to a valid search warrant; pursuant to court-ordered parole or probation conditions, if applicable; 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 tracking 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.

### 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. 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 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

Data is stored electronically by the host company for 90 days, and then it is purged.

Printed data 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) trackers are devices designed to track the movements of vehicles, bicycles, cargo, machinery, and/or individuals.

The Berkeley Police Department currently uses two types of GPS Tracking Devices. The manufacturer, 3SI Security System, 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 - per the manufacturer.
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

The purpose of GPS trackers is to enhance the quality of active investigations. The trackers are utilized during active investigations and shall be used pursuant to a lawfully issued search warrant, court order, or with consent as described below.

### 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. 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 unauthorized use of its data. The 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.

### 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

Location data is obtained through the use of a GPS Tracker.

Latitude and longitude data is captured and stored indefinitely by 3SI when both types of trackers are used. This data is only shared with the District Attorney's Office for prosecution purposes.

#### G. DATA SECURITY

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. In addition, Captains for Divisions utilizing 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

None.

#### K. EXPERIENCE OF OTHER ENTITIES

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

## Surveillance Use Policy - ALPR

### 1302.1 PURPOSE

This Surveillance Use Policy is issued in compliance with BMC 2.99, and incorporates 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 in conjunction with any routine 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 and Berkeley Police Department policy. (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 Department of Information Technology (IT) and associated ALPR system providers/vendors as identified in Appendix A. 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 requester 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.

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 (a))

#### **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.

**DRAFT**



## 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 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 OPERATIONS**

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 shall only be used for official law enforcement business.
  - (b) An ALPR may be used in conjunction with any routine 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.
  - (d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
  - (e) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.
  - (f) If practicable, the officer should verify an ALPR response through the California Law 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 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.

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 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.

---

#### **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 requester 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.

---

(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).

#### **422.8 GENERAL PARKING AND SCOFFLAW ENFORCEMENT**

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 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.

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:

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.

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.

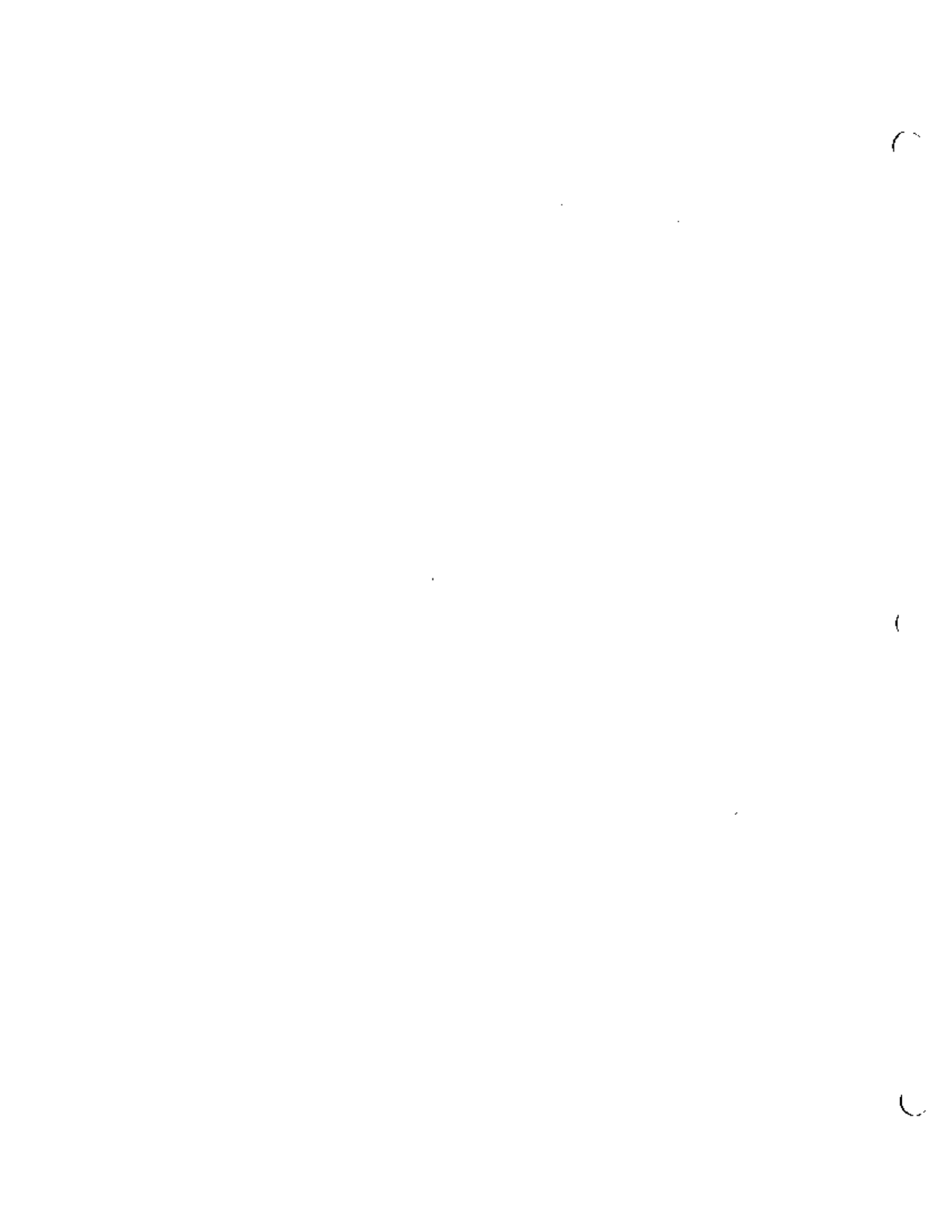
The contracted vendor for the City's Parking Enforcement ALPR is currently Genetec. The city uses Genetec ALPRs to support efficient enforcement of posted time limit parking and Residential Preferential Parking permits.

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.



---

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.



DEPARTMENT ORDER

ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

**SUBJECT: AUTOMATED LICENSE PLATE READER (ALPR)**

PURPOSE

- 1 - This order establishes guidelines for the use of the Berkeley Police Department's Automated License Plate Reader (ALPR) technology and data. ALPR technology functions by automatically capturing an image of a vehicle's license plate, transforming that image into alphanumeric characters using optical character recognition software, and storing that information, along with relevant metadata (e.g. geo-location and temporal information, as well as data about the ALPR). ALPRs may be used by the Berkeley Police Department Parking Enforcement and Traffic Units for official law enforcement purposes.

POLICY

**Administration of ALPR Data**

- 2- Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain through the Traffic Bureau. The Investigations Division Captain will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

**ALPR Operation**

- 3- Department personnel shall not use, or allow others to use, the ALPR equipment or database records for any unauthorized purpose.
  - a. An ALPR shall only be used for official and legitimate law enforcement business.
  - b. Reasonable suspicion or probable cause is not required before using an ALPR.
  - c. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
  - d. No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.

## DEPARTMENT ORDER

ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

---

### ALPR Data Collection and Retention

- 4- 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.
- 5- The Parking Enforcement Manager is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by City Department of Information Technology personnel 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.
- 6- All ALPR data shall be stored as described in this order and thereafter shall 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 shall be downloaded from the server onto portable media and booked into evidence. The records will then be subject to standard evidence retention policies and statutes.
  - 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.

### Accountability and Safeguards

- 7- 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:
  - a. Non-law enforcement requests for access to stored ALPR data shall be processed according to General Order R-23 in accordance with applicable law.
  - b. Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requestor is the registered owner of the vehicle in question, and when providing such

## DEPARTMENTAL ORDER

ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

---

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. 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.
- d. Berkeley Police personnel 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 relates to a specific criminal investigation or department-related civil or administrative action and parking enforcement.
- e. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes only in connection with specific criminal investigations.
- f. 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.
- g. Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units are marked, corrected, or deleted in accordance with the type and severity of the error in question.
- h. ALPR system audits will be conducted by personnel assigned to the Professional Standards Bureau on a regular basis, at least biennially.

### **Current ALPR Deployments**

- 9- The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for parking and scofflaw enforcement.
- 10- Effective 2/18/16, the Parking Enforcement Unit will utilize five (5) Parking Enforcement Go-4 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/SVS database (stolen and wanted vehicles). The

## DEPARTMENTAL ORDER

ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

---

current contracted vendor for this system is PCS Mobile using Genetec ALPR technology.

- 11- The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates, and checks scanned "reads" against a file 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 and penalties. ALPR equipment is installed in the Parking Enforcement Unit's Scofflaw Enforcement vehicle.
- 12- 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.
- 13- 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.
- 14- 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

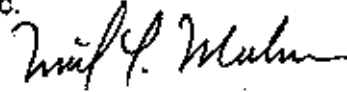
DEPARTMENTAL ORDER

ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

---

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



Michael K. Meehan  
Chief of Police

References: NCRIC ALPR Policy  
SB 34  
General Order R-23

Cc: All BPD Personnel

