PENAL CODE
SECTION 630-638

630. The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

The Legislature by this chapter intends to protect the right of privacy of the people of this state.

The Legislature recognizes that law enforcement agencies have a legitimate need to employ modern listening devices and techniques in the investigation of criminal conduct and the apprehension of lawbreakers. Therefore, it is not the intent of the Legislature to place greater restraints on the use of listening devices and techniques by law enforcement agencies than existed prior to the effective date of this chapter.

631. (a) Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both a fine and imprisonment in the county jail or pursuant to subdivision (h) of Section 1170. If the person has previously been convicted of a violation of this section or Section 632, 632.5, 632.6, 632.7, or 636, he or she is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both that fine and imprisonment.

(b) This section shall not apply (1) to any public utility engaged in the business of providing communications services and facilities, or to the officers, employees or agents thereof, where the acts otherwise prohibited herein are for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility, or (2) to the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a

public utility, or (3) to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(c) Except as proof in an action or prosecution for violation of this section, no evidence obtained in violation of this section shall be admissible in any judicial, administrative, legislative, or other proceeding.

(d) This section shall become operative on January 1, 1994.

632. (a) Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500), or imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has previously been convicted of a violation of this section or Section 631, 632.5, 632.6, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars ($10,000), by imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(b) The term "person" includes an individual, business association, partnership, corporation, limited liability company, or other legal entity, and an individual acting or purporting to act for or on behalf of any government or subdivision thereof, whether federal, state, or local, but excludes an individual known by all parties to a confidential communication to be overhearing or recording the communication.

(c) The term "confidential communication" includes any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.

(d) Except as proof in an action or prosecution for violation of this section, no evidence obtained as a result of eavesdropping upon or recording a confidential communication in violation of this section shall be admissible in any judicial, administrative, legislative, or other proceeding.

(e) This section does not apply (1) to any public utility engaged in the business of providing communications services and facilities, or to the officers, employees or agents thereof, where the acts otherwise prohibited by this section are for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility, or (2) to the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility, or (3) to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(f) This section does not apply to the use of hearing aids and similar devices, by persons afflicted with impaired hearing, for the purpose of overcoming the impairment to permit the hearing of sounds ordinarily audible to the human ear.

632.5. (a) Every person who, maliciously and without the consent of all parties to the communication, intercepts, receives, or assists in intercepting or receiving a communication transmitted between cellular radio telephones or between any cellular radio telephone and a landline telephone shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500), by imprisonment in the county jail not exceeding one year or in the state prison, or by both that fine and imprisonment. If the person has been previously convicted of a violation of this section or Section 631, 632, 632.6, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars ($10,000), by imprisonment in the county jail not exceeding one year or in the state prison, or by both that fine and imprisonment.

(b) In the following instances, this section shall not apply:

(1) To any public utility engaged in the business of providing communications services and facilities, or to the officers, employees, or agents thereof, where the acts otherwise prohibited are for the purpose of construction, maintenance, conduct, or operation of the services and facilities of the public utility.

(2) To the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of the public utility.

(3) To any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(c) As used in this section and Section 635, "cellular radio telephone" means a wireless telephone authorized by the Federal Communications Commission to operate in the frequency bandwidth reserved for cellular radio telephones.

632.6. (a) Every person who, maliciously and without the consent of all parties to the communication, intercepts, receives, or assists in intercepting or receiving a communication transmitted between cordless telephones as defined in subdivision (c), between any cordless telephone and a landline telephone, or between a cordless telephone and a cellular telephone shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500), by imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has been convicted previously of a violation of Section 631, 632, 632.5, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(b) This section shall not apply in any of the following instances:

(1) To any public utility engaged in the business of providing communications services and facilities, or to the officers, employees, or agents thereof, where the acts otherwise prohibited are for the purpose of construction, maintenance, conduct, or operation of the services and facilities of the public utility.

(2) To the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of the public utility.

(3) To any telephonic communications system used for communication exclusively within a state, county, city and county, or city correctional facility.

(c) As used in this section and in Section 635, "cordless

telephone" means a two-way low power communication system consisting of two parts--a "base" unit which connects to the public switched telephone network and a handset or "remote" unit--which are connected by a radio link and authorized by the Federal Communications Commission to operate in the frequency bandwidths reserved for cordless telephones.

632.7. (a) Every person who, without the consent of all parties to a communication, intercepts or receives and intentionally records, or assists in the interception or reception and intentional recordation of, a communication transmitted between two cellular radio telephones, a cellular radio telephone and a landline telephone, two cordless telephones, a cordless telephone and a landline telephone, or a cordless telephone and a cellular radio telephone, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has been convicted previously of a violation of this section or of Section 631, 632, 632.5, 632.6, or 636, the person shall be punished by a fine not exceeding ten thousand dollars ($10,000), by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(b) This section shall not apply to any of the following:

(1) Any public utility engaged in the business of providing communications services and facilities, or to the officers, employees, or agents thereof, where the acts otherwise prohibited are for the purpose of construction, maintenance, conduct, or operation of the services and facilities of the public utility.

(2) The use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of the public utility.

(3) Any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(c) As used in this section, each of the following terms have the following meaning:

(1) "Cellular radio telephone" means a wireless telephone authorized by the Federal Communications Commission to operate in the frequency bandwidth reserved for cellular radio telephones.

(2) "Cordless telephone" means a two-way, low power communication system consisting of two parts, a "base" unit which connects to the public switched telephone network and a handset or "remote" unit, that are connected by a radio link and authorized by the Federal Communications Commission to operate in the frequency bandwidths reserved for cordless telephones.

(3) "Communication" includes, but is not limited to, communications transmitted by voice, data, or image, including facsimile.

633. Nothing in Section 631, 632, 632.5, 632.6, or 632.7 prohibits the Attorney General, any district attorney, or any assistant, deputy, or investigator of the Attorney General or any district attorney, any officer of the California Highway Patrol, any chief of police, assistant chief of police, or police officer of a city or city and county, any sheriff, undersheriff, or deputy sheriff regularly employed and paid in that capacity by a county, police officer of the County of Los Angeles, or any person acting pursuant to the direction of one of these law enforcement officers acting

within the scope of his or her authority, from overhearing or recording any communication that they could lawfully overhear or record prior to the effective date of this chapter.

Nothing in Section 631, 632, 632.5, 632.6, or 632.7 renders inadmissible any evidence obtained by the above-named persons by means of overhearing or recording any communication that they could lawfully overhear or record prior to the effective date of this chapter.

633.05. (a) Nothing in Section 632, 632.5, 632.6, or 632.7 prohibits a city attorney acting under authority of Section 41803.5 of the Government Code, provided that authority is granted prior to January 1, 2012, or any person acting pursuant to the direction of one of those city attorneys acting within the scope of his or her authority, from overhearing or recording any communication that they could lawfully overhear or record.

(b) Nothing in Section 632, 632.5, 632.6, or 632.7 renders inadmissible any evidence obtained by the above-named persons by means of overhearing or recording any communication that they could lawfully overhear or record.

633.1. (a) Nothing in Section 631, 632, 632.5, 632.6, or 632.7 prohibits any person regularly employed as an airport law enforcement officer, as described in subdivision (d) of Section 830.33, acting within the scope of his or her authority, from recording any communication which is received on an incoming telephone line, for which the person initiating the call utilized a telephone number known to the public to be a means of contacting airport law enforcement officers. In order for a telephone call to be recorded under this subdivision, a series of electronic tones shall be used, placing the caller on notice that his or her telephone call is being recorded.

(b) Nothing in Section 631, 632, 632.5, 632.6, or 632.7 renders inadmissible any evidence obtained by an officer described in subdivision (a) if the evidence was received by means of recording any communication which is received on an incoming public telephone line, for which the person initiating the call utilized a telephone number known to the public to be a means of contacting airport law enforcement officers.

(c) This section shall only apply to airport law enforcement officers who are employed at an airport which maintains regularly scheduled international airport service and which maintains permanent facilities of the United States Customs Service.

633.5. Nothing in Section 631, 632, 632.5, 632.6, or 632.7 prohibits one party to a confidential communication from recording the communication for the purpose of obtaining evidence reasonably believed to relate to the commission by another party to the communication of the crime of extortion, kidnapping, bribery, any felony involving violence against the person, or a violation of Section 653m. Nothing in Section 631, 632, 632.5, 632.6, or 632.7 renders any evidence so obtained inadmissible in a prosecution for extortion, kidnapping, bribery, any felony involving violence against the person, a violation of Section 653m, or any crime in connection therewith.

633.6. (a) Notwithstanding the provisions of this chapter, and in accordance with federal law, upon the request of a victim of domestic violence who is seeking a domestic violence restraining order, a judge issuing the order may include a provision in the order that permits the victim to record any prohibited communication made to him or her by the perpetrator.

(b) The Judicial Council shall amend its domestic violence prevention application and order forms to incorporate the provisions of this section.

633.8. (a) It is the intent of the Legislature in enacting this section to provide law enforcement with the ability to use electronic amplifying or recording devices to eavesdrop on and record the otherwise confidential oral communications of individuals within a location when responding to an emergency situation that involves the taking of a hostage or the barricading of a location. It is the intent of the Legislature that eavesdropping on oral communications pursuant to this section comply with paragraph (7) of Section 2518 of Title 18 of the United States Code.

(b) Notwithstanding the provisions of this chapter, and in accordance with federal law, a designated peace officer described in subdivision (c) may use, or authorize the use of, an electronic amplifying or recording device to eavesdrop on or record, or both, any oral communication within a particular location in response to an emergency situation involving the taking of a hostage or hostages or the barricading of a location if all of the following conditions are satisfied:

(1) The officer reasonably determines that an emergency situation exists involving the immediate danger of death or serious physical injury to any person, within the meaning of Section 2518(7)(a)(i) of Title 18 of the United States Code.

(2) The officer reasonably determines that the emergency situation requires that the eavesdropping on oral communication occur immediately.

(3) There are grounds upon which an order could be obtained pursuant to Section 2516(2) of Title 18 of the United States Code in regard to the offenses enumerated therein.

(c) Only a peace officer who has been designated by either a district attorney in the county where the emergency exists, or by the Attorney General to make the necessary determinations pursuant to paragraphs (1), (2), and (3) of subdivision (b) may make those determinations for purposes of this section.

(d) If the determination is made by a designated peace officer described in subdivision (c) that an emergency situation exists, a peace officer shall not be required to knock and announce his or her presence before entering, installing, and using any electronic amplifying or recording devices.

(e) If the determination is made by a designated peace officer described in subdivision (c) that an emergency situation exists and an eavesdropping device has been deployed, an application for an order approving the eavesdropping shall be made within 48 hours of the beginning of the eavesdropping and shall comply with the requirements of Section 629.50. A court may grant an application authorizing the use of electronic amplifying or recording devices to eavesdrop on and record otherwise confidential oral communications in

barricade or hostage situations where there is probable cause to believe that an individual is committing, has committed, or is about to commit an offense listed in Section 2516(2) of Title 18 of the United States Code.

(f) The contents of any oral communications overheard pursuant to this section shall be recorded on tape or other comparable device. The recording of the contents shall be done so as to protect the recording from editing or other alterations.

(g) For purposes of this section, a "barricading" occurs when a person refuses to come out from a covered or enclosed position. Barricading also occurs when a person is held against his or her will and the captor has not made a demand.

(h) For purposes of this section, a "hostage situation" occurs when a person is held against his or her will and the captor has made a demand.

(i) A judge shall not grant an application made pursuant to this section in anticipation that an emergency situation will arise. A judge shall grant an application authorizing the use of electronic amplifying or recording devices to eavesdrop on and record otherwise confidential oral communications in barricade or hostage situations where there is probable cause to believe that an individual is committing, has committed, or is about to commit an offense listed in Section 2516(2) of Title 18 of the United States Code, and only if the peace officer has fully complied with the requirements of this section. If an application is granted pursuant to this section, an inventory shall be served pursuant to Section 629.68.

(j) This section does not require that a peace officer designated pursuant to subdivision (c) undergo training pursuant to Section 629.94.

(k) A peace officer who has been designated pursuant to subdivision (c) to use an eavesdropping device shall cease use of the device upon the termination of the barricade or hostage situation, or upon the denial by a judge of an application for an order to approve the eavesdropping, whichever is earlier.

(l) Nothing in this section shall be deemed to affect the admissibility or inadmissibility of evidence.

634. Any person who trespasses on property for the purpose of committing any act, or attempting to commit any act, in violation of Section 631, 632, 632.5, 632.6, 632.7, or 636 shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500), by imprisonment in the county jail not exceeding one year or in the state prison, or by both that fine and imprisonment. If the person has previously been convicted of a violation of this section or Section 631, 632, 632.5, 632.6, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars ($10,000), by imprisonment in the county jail not exceeding one year or in the state prison, or by both that fine and imprisonment.

635. (a) Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of

Model Policy

	Effective Date **April 2014**	***Number***
Subject **Body-Worn Cameras**		
Reference		***Special Instructions***
Distribution	***Reevaluation Date***	***No. Pages*** **3**

I. PURPOSE

This policy is intended to provide officers with instructions on when and how to use body-worn cameras (BWCs) so that officers may reliably record their contacts with the public in accordance with the law.[1]

II. POLICY

It is the policy of this department that officers shall activate the BWC when such use is appropriate to the proper performance of his or her official duties, where the recordings are consistent with this policy and law. This policy does not govern the use of surreptitious recording devices used in undercover operations.

III. PROCEDURES

A. Administration

This agency has adopted the use of the BWC to accomplish several objectives. The primary objectives are as follows:

1. BWCs allow for accurate documentation of police-public contacts, arrests, and critical incidents. They also serve to enhance the accuracy of officer reports and testimony in court.
2. Audio and video recordings also enhance this agency's ability to review probable cause for arrest, officer and suspect interaction, and evidence for investigative and prosecutorial purposes and to provide additional information for officer evaluation and training.
3. The BWC may also be useful in documenting crime and accident scenes or other events that include the confiscation and documentation of evidence or contraband.

B. When and How to Use the BWC

1. Officers shall activate the BWC to record all contacts with citizens in the performance of official duties.
2. Whenever possible, officers should inform individuals that they are being recorded. In locations where individuals have a reasonable expectation of privacy, such as a residence, they may decline to be recorded unless the recording is being made in pursuant to an arrest or search of the residence or the individuals. The BWC shall remain activated until the event is completed in order to ensure the integrity of the recording unless the contact moves into an area restricted by this policy (see items D.1-4).
3. If an officer fails to activate the BWC, fails to record the entire contact, or interrupts the recording, the officer shall document why a recording was not made, was interrupted, or was terminated.
4. Civilians shall not be allowed to review the recordings at the scene.

C. Procedures for BWC Use

1. BWC equipment is issued primarily to uniformed personnel as authorized by this agency. Officers who are assigned BWC equipment must use the equipment unless otherwise authorized by supervisory personnel.
2. Police personnel shall use only BWCs issued by

this department. The BWC equipment and all data, images, video, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of the agency.

3. Police personnel who are assigned BWCs must complete an agency approved and/or provided training program to ensure proper use and operations. Additional training may be required at periodic intervals to ensure the continued effective use and operation of the equipment, proper calibration and performance, and to incorporate changes, updates, or other revisions in policy and equipment.
4. BWC equipment is the responsibility of individual officers and will be used with reasonable care to ensure proper functioning. Equipment malfunctions shall be brought to the attention of the officer's supervisor as soon as possible so that a replacement unit may be procured.
5. Officers shall inspect and test the BWC prior to each shift in order to verify proper functioning and shall notify their supervisor of any problems.
6. Officers shall not edit, alter, erase, duplicate, copy, share, or otherwise distribute in any manner BWC recordings without prior written authorization and approval of the chief executive officer (CEO) or his or her designee.
7. Officers are encouraged to inform their supervisor of any recordings that may be of value for training purposes.
8. If an officer is suspected of wrongdoing or involved in an officer-involved shooting or other serious use of force, the department reserves the right to limit or restrict an officer from viewing the video file.
9. Requests for deletion of portions of the recordings (e.g., in the event of a personal recording) must be submitted in writing and approved by the chief executive officer or his or her designee in accordance with state record retention laws. All requests and final decisions shall be kept on file.
10. Officers shall note in incident, arrest, and related reports when recordings were made during the incident in question. However, BWC recordings are not a replacement for written reports.

D. Restrictions on Using the BWC

BWCs shall be used only in conjunction with official law enforcement duties. The BWC shall not generally be used to record:

1. Communications with other police personnel without the permission of the chief executive officer (CEO);
2. Encounters with undercover officers or confidential informants;
3. When on break or otherwise engaged in personal activities; or
4. In any location where individuals have a reasonable expectation of privacy, such as a restroom or locker room.

E. Storage

1. All files[2] shall be securely downloaded periodically and no later than the end of each shift. Each file shall contain information related to the date, BWC identifier, and assigned officer.
2. All images and sounds recorded by the BWC are the exclusive property of this department. Accessing, copying, or releasing files for non law enforcement purposes is strictly prohibited.
3. All access to BWC files must be specifically authorized by the CEO or his or her designee, and all access is to be audited to ensure that only authorized users are accessing the data for legitimate and authorized purposes.
4. Files should be securely stored in accordance with state records retention laws and no longer than useful for purposes of training or for use in an investigation or prosecution. In capital punishment prosecutions, recordings shall be kept until the offender is no longer under control of a criminal justice agency.

F. Supervisory Responsibilities

1. Supervisory personnel shall ensure that officers equipped with BWC devices utilize them in accordance with policy and procedures defined herein.
2. At least on a monthly basis, supervisors will randomly review BWC recordings to ensure that the equipment is operating properly and that officers are using the devices appropriately and in accordance with policy and to identify any areas in which additional training or guidance is required.

END NOTES

[1] Some states have eavesdropping statutes that require two-party consent prior to audio recording. Consult your legal advisor for state and local laws that affect your agency.

[2] For the purpose of this document, the term "file" refers to all sounds, images, and associated metadata.

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this model policy incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities among other factors.

This project was supported by Grant No. 2010-DJ-BX-K002 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or the IACP.

IACP National Law Enforcement Policy Center Staff: Philip Lynn, Manager; Sara Dziejma, Project Specialist; and Vincent Talucci, Executive Director,International Association of Chiefs of Police.

IACP NATIONAL LAW ENFORCEMENT POLICY CENTER

Body-Worn Cameras

Concepts and Issues Paper

April 2014

I. INTRODUCTION

A. Purpose of the Document

This paper is designed to accompany the *Model Policy on Body-Worn Cameras* published by the IACP National Law Enforcement Policy Center. This paper provides essential background material and supporting documentation to provide a greater understanding of the developmental philosophy and implementation requirements for the model policy. This material will be of value to law enforcement executives in their efforts to tailor the model to the requirements and circumstances of their communities and their law enforcement agencies.

B. Background

Video recorders and digital cameras have been useful tools in the law enforcement profession for some years. Advances in technology have improved camera equipment and enhanced the development of the body-worn camera (BWC). While many police agencies have taken advantage of these advancements even more have overlooked or are unaware of their usefulness, or have chosen not to deploy them.

The concept of recording police-citizen encounters for law enforcement use first developed with the implementation of in-car cameras. Initially, these devices were installed to document interactions with individuals suspected of driving under the influence, with the recordings providing supporting evidence needed for conviction.[1] Over time, agencies discovered that in-car cameras had numerous additional benefits, such as "increased officer safety; documentation of traffic violations, citizen behavior, and other events; reduced court time and prosecutor burden; video evidence for use in internal investigations; reduced frivolous lawsuits; and increased likelihood of successful prosecution."[2] All of these advantages also apply to the BWC, as will be discussed further in this document.

C. Uses for Body-Worn Cameras

Many police officers now use BWCs to document interactions with victims, witnesses, and others during police-citizen encounters, at crime and incident scenes, and during traffic stops. In many instances police agencies have found the BWC useful for officers in the favorable resolution of both administrative and criminal complaints and as a defense resource in cases of civil liability. Officers using these recorders have a clearly documented, firsthand, completely objective account of what was said during an incident in question. The utilization of BWC video and audio recordings at trial can provide the court with the actual statements of officers, suspects, and others that might not otherwise be admissible in court based upon hearsay concerns, or might not get sufficient consideration if there are conflicting memories of the statements. In addition, recordings made at crime and incident scenes are a tangible benefit of BWCs and can provide investigators, prosecutors, and juries with far more detailed, accurate, and compelling evidence.

The use of BWCs gives officers, their agencies, administrators, and employing jurisdictions an additional means of defending themselves in civil litigation. This is extremely useful in resolving citizen complaints and potential civil actions. During many police-citizen contacts there are no objective witnesses to corroborate either allegations of misfeasance or explanations of the interaction and so many jurisdictions are more willing to resolve these matters by paying minor damages rather than spend time and money in litigation. However, an officer utilizing a BWC

A publication of the IACP National Law Enforcement Policy Center
44 Canal Center Plaza, Suite 200, Alexandria, VA 22314

typically has all the comments and actions of both parties on record and thus has a built-in "impartial witness" on his or her person—a factor that has often resulted in civil suits before they would otherwise have been formally lodged. In one study of in-car camera recordings, "in cases where video evidence was available, the officer was exonerated 93% of the time; in 5% of the cases the complaint was sustained."[3] In addition, the same study showed that in a large number of instances, the individual decided against filing a complaint once he or she was notified that there was a video recording of the incident.[4]

The BWC has also proven to be effective in helping police agencies evaluate police officer performance in a more complete and fair manner. Supervisory personnel are able to review officer conduct and performance on a random or systematic basis by reviewing BWC recordings. This allows the supervisor to ensure that the BWC is being used in accordance with department policy and to identify any areas in which additional officer training, guidance, or discipline may be required.

Introduction and subsequent broad acceptance of in-car mobile video recording equipment has played a significant role in proving the effectiveness and utility of recording equipment in law enforcement. However, vehicle-mounted video recorders are limited in their field of vision and are not of assistance to officers on foot patrol or who are engaged in investigations or interactions beyond transmission range of their vehicles. The BWC is a convenient and relatively inexpensive means of more fully documenting contacts and interactions with citizens, suspects, and others in a wide variety of situations. It gives them a reliable and compact tool to systematically and automatically record their field observations and encounters.

However, in most cases BWCs should not be viewed as a low-cost alternative to in-car video recorders, but rather a complementary technology. In-car camera systems can provide important information that is currently unavailable with BWCs. For instance, most in-car camera systems can be linked to vehicle systems and record vehicle location, speed, application of brakes; indicate activation of lights and siren; and capture other data that could be vitally important if an accident or other unanticipated event should occur. For example, recording of an officer's activity from the patrol car often includes accidents that occur during a traffic stop that would not necessarily be seen by the BWC while the officer interacts with the motorist. Most in-car systems also provide the option of installing a secondary camera to record any activity in the back seat of the patrol car.

Police officers are aware that contact with citizens during routine traffic stops or in other types of police-public interactions can result in confrontational situations. It has been the experience of many officers who have been in potentially hostile or confrontational situations and who are equipped with audio or video recording devices that inform the subject that he or she is being recorded by one or both of these means often serves to de-escalate or defuse the situation. The subject realizes in these situations that his or her statements cannot be denied or refuted later because there is a recording documenting every aspect of the encounter. The same concept can be applied to officer behavior. In a one-year study conducted by the Rialto, California, Police Department, citizen complaints of officer misconduct fell by 87.5 percent for officers using BWCs, while uses of force by such officers fell by 59 percent.[5]

Finally, the availability of video and audio recordings as evidence is critically important and can be the key to successful prosecution. For example, there is often nothing more compelling to a judge or jury than actually seeing the actions and hearing the words uttered by a suspect, including statements of hostility and anger.

Throughout the United States, courts are backlogged with cases waiting to be heard and officers who are spending time in court that could be used more productively in enforcement activities. The availability of audio and/or video recorded evidence increases the ability of prosecutors to obtain guilty verdicts more easily and quickly at trial or to more effectively plea-bargain cases, avoiding lengthy trial proceedings. In jurisdictions that employ audio and visual evidence, officers normally submit their recordings along with a written report, which is later reviewed by the prosecuting attorney. When the accused and his or her attorney are confronted with this evidence, guilty pleas are more often obtained without the need for a trial or the pressure to accept a plea to lesser charges. This substantially reduces the amount of time an officer must spend in court and utilizes prosecutorial and judicial resources more efficiently.

II. ADMINISTRATIVE RESTRICTIONS ON BODY-WORN CAMERA RECORDINGS

The usefulness of BWCs has been clearly demonstrated; however, their utility is realized only when they are recording. Agency policy should require that officers activate their BWC whenever they make contact with a citizen in the course of conducting official police business. Once activated, the entire conversation should be recorded without interruption. If such interruption occurs, the officer should be required to document the reason for the interruption in a report. If an officer feels it is necessary to stop recording (e.g., while speaking to another officer, or a confidential informant) within constraints of policy, he or she may also be permitted to verbally indicate his or her intent to stop the recording before stopping the device,

and upon reactivation, state that he or she has restarted the recording. This will help avoid accusations of editing the recording after the fact.

Some agencies issue BWCs to select officers rather than to all patrol officers. This approach can be used as part of an effort to more closely monitor individual officers who are suspected of having difficulty in certain areas of operation. Or it may simply be that a department cannot afford to provide cameras for all personnel. However, issuing cameras for the sole purpose of monitoring specific employees can have several negative consequences. For example, officers who know they are under close scrutiny may tend to modify their behavior only while the BWC is deployed. Selective use of BWCs can also be stigmatizing, since the officer's colleagues may interpret that he or she is being singled out as a potential problem. This can have negative short- and long-term consequences for the subject officer in dealing effectively and professionally thereafter with fellow officers. Such selective use can also be a considerable impediment to creating "buy in" from employees regarding the use and utility of video recorders. If officers regard these devices primarily as monitors for identifying problem behavior, they will be less likely to use them for the purpose they are intended. Therefore, it is strongly recommended that agencies using BWCs for patrol personnel should provide them to all such officers for use in accordance with agency policy.

In spite of their utility, the BWCs can be used for improper purposes that are counter to or inconsistent with the law enforcement mission, or in ways that are contrary to federal, state, or local law. For example, BWCs are not meant to serve personal uses whether on or off duty unless permission is granted by the department. This is a simple matter of concern over private use of governmental equipment in most cases, but it can also involve concerns over the potential of mixing personal recordings with those involving official police business. In the latter circumstances, the evidentiary integrity of recordings could be called into question, as could issues surrounding the chain of custody of evidence contained on devices that may have been involved in personal use. Personal use of BWC equipment and comingling of recordings raise concerns about inappropriate viewing, sharing, and release of videos and associated issues of invasion of privacy and other similar types of liability.

In general, BWCs should be used for investigative purposes or field use only and should not be activated in administrative settings. Another potential for improper use that should be prohibited by the police department is surreptitious recording of communications with or between any other officers without the explicit permission of the agency chief executive or his or her designee. The purposeful activation of BWCs during personal conversations involving counseling, guidance sessions, or personnel evaluations should be prohibited unless all parties present agree to be recorded. It is important to note the dysfunction and disharmony created by surreptitious recordings in a police work environment. A cloud of suspicion and distrust exists where officers and their supervisors believe that they cannot enter into candid personal discussions without the risk of their statements being recorded and used inappropriately or harmfully against them or others. The result can undermine both the willingness of supervisors and administrators to provide candid guidance about officer performance, and the willingness of employees to provide open, truthful information.

Similarly, officers' conversations on the radio and among each other at a scene will frequently occur. Officers should inform other officers or emergency responders arriving on a scene when their recorder is active to help avoid recording inappropriate or immaterial statements. In addition, the BWC should not be activated when the officer is on break or otherwise engaged in personal activities or when the officer is in a location where there is a reasonable expectation of privacy, such as a restroom or locker room. For safety and confidentiality reasons, encounters with undercover officers or confidential informants should not be recorded.

The policy should clearly state that BWC activation is limited to situations involving official police activities authorized by law or court order, including consensual citizen encounters and investigation of law violations. Failure to follow this policy could subject an officer to disciplinary action up to and including dismissal.

A. Legal Restrictions on Recordings

As noted in the foregoing section, the availability and use of BWCs can create the basis for legal challenges lodged by suspects or other persons. This policy applies only to the use of BWCs attached to an officer's person, and any use of the camera in a surreptitious manner by removing it and using it to monitor a situation remotely should be strictly controlled. Such surreptitious recording has constitutional implications and may be governed by state and federal wiretap laws not applicable to or addressed by this policy. It is important for officers who are equipped with BWCs to have an understanding of the restrictions on surreptitious recording of persons and to make sure their use of the BWCs is consistent with the restrictions.

This policy is intended to cover use of BWCs in situations where a person has either a reduced or no expectation of privacy and that occurs in a place where the officer is legally entitled to be present. Whether there is a reasonable expectation of privacy in a given situation is determined

using a traditional Fourth Amendment analysis involving whether the person in question exhibited "an actual or subjective expectation of privacy" in the communication and whether that expectation is "one that society is prepared to recognize as reasonable." The landmark U.S. Supreme Court decision in *Katz v. United States*[6] that outlined these principles also made it clear that a reasonable expectation of privacy is not determined so much by the place in which the individual is located (e.g., a telephone booth, business office, or taxicab) but by what a person "seeks to preserve as private even in an area accessible to the public." The decision emphasized that the Fourth Amendment protects people, not places.

When an individual is in custody, whether in a patrol car, interrogation room, or lockup, for example, there is generally no reasonable expectation of privacy, unless the suspect is speaking in confidence with an attorney, clergyman or other individual with privilege of communication. Recording may be done in these settings unless officers have given the individual a sign or indication that the location is private, that their conversation is not being recorded, and/or if the individual is speaking with someone with privilege. Individuals who are in these settings, but who are not in custody may refuse to be recorded.

In a residence, there is a heightened degree and expectation of privacy. Officers should normally inform the resident that he or she is being recorded. If the resident wishes not to be recorded, this request should be documented by recording the request before the device is turned off. However, if an officer may enter a dwelling without the consent of the resident, such as when serving a warrant, or when the officer is there based on an exception to the warrant requirement, recordings should be made of the incident until its conclusion. As a general rule, if the officer must legally ask permission to enter a premises, he or she should also ask if the resident will allow recording.

Notwithstanding any legal limitations, as a courtesy and so as not to create the impression of trickery or subterfuge, some police agencies require their officers to inform all persons who are being recorded by BWCs. This includes all motor vehicle stops and related citizen contacts where official police functions are being pursued.

Recording arrests and the events leading up to an arrest is an excellent means of documenting the circumstances establishing probable cause for arrest. In circumstances where *Miranda* rights are appropriate, use of BWCs is a good way to demonstrate the clear and accurate reading of *Miranda* rights to the suspect—and an invocation or waiver of those rights by the suspect. If the suspect invokes his or her rights to silence and representation by an attorney, recording is still permissible. Officers should take great care not to direct questions to the suspect regarding involvement in any crime. However, any spontaneous statements made by the suspect to officers would likely be admissible as evidence so long as the statements or comments were not elicited by officer questioning.

Finally, there may be times when officers should be given a degree of discretion to discontinue recording in sensitive situations as long as they record the reason for deactivating the recorded. For instance, when talking to a sexual assault victim, or on the scene of a particularly violent crime or accident scene. This is especially true if the recording may be subject to Freedom of Information Act requests. Under such circumstances, recordings could be posted on media sites that could cause unnecessary distress for families and relatives. Whenever reasonably possible, officers should also avoid recording children who are not involved in an incident as well as innocent bystanders.

B. Procedures for Using Body-Worn Cameras

BWC equipment is intended primarily for the use of uniformed officers although plainclothes officers may be issued such equipment. Officers who are assigned such equipment should be required to use it in accordance with agency policy unless otherwise directed or authorized by supervisory personnel.

Personnel who are authorized to use BWCs should use only equipment provided by the department. The chances of loss, destruction, or recording over materials belonging to official police investigations may be greater when these devices are used for both official and personal business.

BWC equipment should be the responsibility of individual officers assigned such equipment and should be used with reasonable care to ensure proper functioning. Equipment malfunctions should be brought to the attention of the officer's supervisor as soon as possible so that a replacement unit may be obtained. Officers should test this equipment prior to each shift in order to verify that it is functioning properly and should notify their supervisor if any problems are detected.

Officers should never erase or in any manner alter recordings. The agency must maintain strict managerial control over all devices and recorded content so that it can ensure the integrity of recordings made by officers. Failure of officers to assist in this effort or the agency to take managerial control over recordings can risk the credibility of the program and threaten its continuation as a source of credible information and evidence.

Where officers have recorded unusual and/or operational situations or incidents that may have potential value in training, they should inform their supervisor so that the recordings can be identified and evaluated. Unusual or even routine events recorded on tape can be used in basic academy and in-service training to reinforce appropriate

behavior and procedures, to demonstrate inappropriate practices and procedures, to enhance interpersonal skills and officer safety habits, and to augment the instructional routines of field training officers and supervisory personnel.

Officers should also note in their incident, arrest, or related reports when recordings were made during the events in question. However, BWC recordings should not serve as a replacement for written reports.

C. Recording Control and Management

Reference has been made previously to the need for control and management of BWC recordings to ensure the integrity of the recordings, secure the chain of custody where information of evidentiary value is obtained, and use recordings to their fullest advantage for training and other purposes. In order to accomplish these ends, officers and their supervisors should adhere to a number of procedural controls and requirements.

At the end of each shift, all files from the BWC should be securely downloaded. In order for a recording to be admissible in court, the officer must be able to authenticate the recording as a true and accurate depiction of the events in question. In an effort to prevent the recording from becoming evidence, the defense may question the chain of custody. Therefore, departments may wish to utilize secure downloading software or programs, or have an individual other than the officer be responsible for downloading the data in an effort to minimize any chain-of-custody issues.[7]

Each file should contain identifying information, such as the date, time, BWC device used, and assigned officer. These recordings should be stored in a secure manner and are the exclusive property of the department. Accessing, copying, or releasing files for non-criminal justice purposes should be strictly prohibited.

Many states have laws specifying how long evidence and other records must be maintained. Recordings should be maintained in a secure manner for the period of time required by state law or as otherwise designated by the law enforcement agency. Retention schedules for recordings should take into consideration the possibility of a civilian complaint against an officer sometime after the encounter. Recordings in these situations can prove invaluable in resolution of the complaint. However, storage costs can become prohibitive, so agencies must balance the need for retaining unspecified recordings with the desire to have this information available.

According to the *Model Policy*, supervisory officers should ensure that officers equipped with BWCs use them in accordance with agency policy and procedures. One means of accomplishing this end is for first-line supervisors to review recordings of officers on their shift. This can be done on a random selection basis or on a systematic basis and should be performed routinely at least monthly. Recordings submitted by specific officers may need to be reviewed more often or more closely should there be indications that the officer's performance is substandard, if there have been internal or external complaints lodged against the officer, or if there is reason to believe that the officer may need additional guidance or training in certain operational areas.

Officers assigned a BWC should have access, and be encouraged to review their own recordings in order to assess their performance and potentially correct unsafe or questionable behaviors. The question of whether an officer should be allowed to review recordings before writing a report, especially following an officer-involved shooting or accident, is a matter that should be examined closely by administrators.

Inevitably, recordings will occur in circumstances where recording is not appropriate. By way of examples, an officer may forget to stop a recording when entering a victim's residence after being asked not to record inside, or may accidentally activate it in the locker room. In these situations, the officer should be afforded an opportunity to request that these portions of the recording be erased. Requests for deletions should be made in writing and must be submitted to the chief executive officer or his or her designee for approval. All requests should be maintained for historical reference.

END NOTES

[1] *The Impact of Video Evidence on Modern Policing*, IACP pg. 5, http://www.cops.usdoj.gov/Publications/video_evidence.pdf (accessed February 12, 2014).

[2] Ibid., pg. 11.

[3] Ibid, pg. 15

[4] Ibid.

[5] As cited in Mesa Arizona Police, *End of Program Evaluation and Recommendations: On-Officer Body Camera System, Axon Flex Program Evaluation and Recommendations*, December 2, 2013, pg. 2.

[6] A touchstone case in this matter is that of *Katz v. United States*, 389 U.S. 347 (1967).

[7] For additional discussion of the use of videotape evidence, please see Jonathan Hak, "Forensic Video Analysis and the Law" appendix v in *The Impact of Video Evidence on Modern Policing*

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this document incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities among other factors.

This project was supported by Grant No. 2010-DJ-BX-K002 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or the IACP.

IACP National Law Enforcement Policy Center Staff: Philip Lynn, Manager; Sara Dziejma, Project Specialist; and Vincent Talucci, Executive Director,International Association of Chiefs of Police.

IACP TECHNOLOGY POLICY FRAMEWORK[1]
January 2014

Introduction

New and emerging technologies increasingly play a crucial role in the daily work of police, equipping officers with enforcement and investigative tools that have the potential of making them safer, better informed, and more effective and efficient. Developing and enforcing comprehensive agency policies regarding deployment and use is a critical step in realizing the value that technologies promise, and is essential in assuring the public that their privacy and civil liberties are recognized and protected.

Technological advances have made it possible to monitor and record nearly every interaction between police and the public through the use of in-car and body-worn video, access to an expanding network of public and private video surveillance systems, and the increasing use of smartphones with digital recording capabilities by citizens and officers alike. Police can track suspects with the use of GPS tracking technologies and officers themselves can be tracked with automated vehicle location (AVL) systems. Automated license plate recognition (ALPR) systems can scan the license plates of vehicles within sight of officers in the field and quickly alert them if the vehicle has been reported stolen or is wanted. Identity can be remotely verified or established with biometric precision using mobile fingerprint scanners and facial recognition software. Crimes can be mapped as they are reported, gunshot detection technology can alert law enforcement almost instantaneously when a firearm is discharged, and surveillance cameras can be programmed to focus in on the gunshot location and stream live video to both dispatchers and responding officers. With these advancements come new opportunities to enhance public and officer safety. They also present new challenges for law enforcement executives.

The challenges include identifying which technologies can be incorporated by the agency to achieve the greatest public safety benefits, and defining metrics that will enable the agency to monitor and assess the value and performance of the technologies. Just because a technology *can* be implemented, does not mean that it *should* be. There are also challenges in integrating these technologies across different platforms, building resilient infrastructure and comprehensive security, providing technical support, and maintaining and upgrading applications and hardware. All of this can be confusing and technically demanding, underscoring the need for effective planning, strategic deployment, and performance management.

Addressing these challenges is paramount because of the broader issues that the use of this expanding array of technologies by law enforcement presents. A principal tenet of policing is the trust citizens grant police to take actions on their behalf. If that trust is violated and public approval lost, police are not able to effectively perform their duties to keep communities safe.

The Policy Mandate

Creating and enforcing agency policies that govern the deployment and use of technology, protecting the civil rights and civil liberties of individuals, as well as the privacy protections afforded to the data collected, stored, and used, is essential to ensure effective and sustainable implementation, and to maintain community trust. Policies function to reinforce training and to establish an operational baseline to guide officers and other personnel in proper procedures regarding its use. Moreover, policies help to ensure uniformity in practice across the agency and to enforce accountability. Policies should reflect the mission and values of the agency and be tightly aligned with applicable local, state, and federal laws, regulations, and judicial rulings.

Policies also function to establish transparency of operations, enabling agencies to allay public fears and misperceptions by providing a framework that ensures responsible use, accountability, and legal and constitutional compliance. The use of automated license plate recognition (ALPR) technologies, unmanned aerial systems, and body-worn video by law enforcement, for example, has generated substantial public discussion, increasing scrutiny, and legislative action in recent years.[2] Privacy advocates, elected officials, and members of the public have raised important questions about how and under what circumstances these technologies are deployed, for what purposes, and how the data gathered by these technologies are retained, used, and shared. Having and enforcing a strong policy framework enables law enforcement executives to demonstrate responsible planning, implementation, and management.

Agencies should adopt and enforce a technology policy framework that addresses technology objectives, deployment, privacy protections, records management, data quality, systems security, data retention and purging, access and use of stored data, information sharing, accountability, training, and sanctions for non-compliance. Agencies should implement safeguards to ensure that technologies will not be deployed in a manner that could violate civil rights (race, religion, national origin, ethnicity, etc.) or civil liberties (speech, assembly, religious exercise, etc.). The policy framework is but one of several critical components in the larger technology planning effort that agencies should undertake to ensure proper and effective use of automation.

Universal Principles

Given the privacy concerns and sensitivity of personally identifiable information and other data often captured and used by law enforcement agencies,[3] and recognizing evolving perceptions of what constitutes a reasonable expectation of privacy,[4] the

technology policy framework should be anchored in principles universally recognized as essential in a democratic society.

The following universal principles should be viewed as a guide in the development of effective policies for *technologies that can, or have the potential to monitor, capture, store, transmit and/or share data, including audio, video, visual images, or other personally identifiable information which may include the time, date, and geographic location where the data were captured*.[5]

1. *Specification of Use*—Agencies should define the purpose, objectives, and requirements for implementing specific technologies, and identify the types of data captured, stored, generated, or otherwise produced.
2. *Policies and Procedures*—Agencies should articulate in writing, educate personnel regarding, and enforce agency policies and procedures governing adoption, deployment, use, and access to the technology and the data it provides. These policies and procedures should be reviewed and updated on a regular basis, and whenever the technology or its use, or use of the data it provides significantly changes.
3. *Privacy and Data Quality*—The agency should assess the privacy risks and recognize the privacy interests of all persons, articulate privacy protections in agency policies, and regularly review and evaluate technology deployment, access, use, data sharing, and privacy policies to ensure data quality (i.e., accurate, timely, and complete information) and compliance with local, state, and federal laws, constitutional mandates, policies, and practice.
4. *Data Minimization and Limitation*—The agency should recognize that only those technologies, and only those data, that are strictly needed to accomplish the specific objectives approved by the agency will be deployed, and only for so long as it demonstrates continuing value and alignment with applicable constitutional, legislative, regulatory, judicial, and policy mandates.
5. *Performance Evaluation*—Agencies should regularly monitor and evaluate the performance and value of technologies to determine whether continued deployment and use is warranted on operational, tactical, and technical grounds.
6. *Transparency and Notice*—Agencies should employ open and public communication and decision-making regarding the adoption, deployment, use, and access to technology, the data it provides, and the policies governing its use. When and where appropriate, the decision-making process should also involve governing/oversight bodies, particularly in the procurement process. Agencies should provide notice, when applicable, regarding the deployment and use of technologies, as well as make their privacy policies available to the public. There are practical and legal exceptions to this principle for technologies that are

lawfully deployed in undercover investigations and legitimate, approved covert operations.[6]

7. *Security*—Agencies should develop and implement technical, operational, and policy tools and resources to establish and ensure appropriate security of the technology (including networks and infrastructure) and the data it provides to safeguard against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. This principle includes meeting state and federal security mandates (e.g., the FBI's CJIS Security Policy[7]), and having procedures in place to respond if a data breach, loss, compromise, or unauthorized disclosure occurs, including whether, how, and when affected persons will be notified, and remedial and corrective actions to be taken.[8]
8. *Data Retention, Access and Use*—Agencies should have a policy that clearly articulates that data collection, retention, access, and use practices are aligned with their strategic and tactical objectives, and that data are retained in conformance with local, state, and/or federal statute/law or retention policies, and only as long as it has a demonstrable, practical value.
9. *Auditing and Accountability*—Agencies and their sworn and civilian employees, contractors, subcontractors, and volunteers should be held accountable for complying with agency, state, and federal policies surrounding the deployment and use of the technology and the data it provides. All access to data derived and/or generated from the use of relevant technologies should be subject to specific authorization and strictly and regularly audited to ensure policy compliance and data integrity. Sanctions for non-compliance should be defined and enforced.

Developing Policies and Operating Procedures

The universal principles provide structural guidance for the development of specific agency policies and operating procedures that comport with established constitutional, legal, and ethical mandates and standards. Agency policies and procedures specify the operational components of each individual technology implementation, deployment, and management, and should typically include and address the following factors:[9]

1. Purpose
    a. A general discussion of the purpose of a specific agency policy to include the agency's position on protecting privacy.
2. Policy
    a. A discussion of the overarching agency policy regarding the deployment and use of a specific technology, its application to members of the agency, and reference to relevant laws, policies, and/or regulations that authorize the agency to implement a technology, or that relate to the use and deployment of a technology.
3. Definitions

a. A description of the technology, its components, and functions.
b. Definitions and acronyms associated with the technology.

4. Management
    a. Strategic Alignment: Describe how the technology aligns and furthers the agency's strategic and tactical deployment objectives.
    b. Objectives and Performance: Identify objectives for the deployment and conditions for use of a technology, and a general strategy for assessing performance and compliance with the agency's policy.
    c. Ownership: Clearly specify that the hardware and software associated with the technology is the property of the agency, regardless whether it has been purchased, leased, or acquired as a service, and that all deployments of a technology are for official use only (FOUO). All data captured, stored, generated, or otherwise produced by a technology are the property of the agency, regardless where the data are housed or stored. All access, use, sharing, and dissemination of the data must comply with the policies established and enforced by the agency.
    d. Classification of Data: Clearly specify the data classification and its level of sensitivity (e.g., top secret, secret, confidential, restricted, unclassified, private, public, etc.), whether the data captured, stored, generated, or otherwise produced by a technology are considered public information, and whether it is subject to applicable public records act requests and under what circumstances.
    e. Privacy Impact: Develop or adopt and use a formal privacy impact assessment (PIA)[10] or similar agency privacy assessment on technology and the data it captures, stores, generates, or otherwise produces.

5. Operations
    a. Installation, Maintenance, and Support: Require regular maintenance, support, upgrades, calibration, and refreshes of a technology to ensure that it functions properly.
    b. Deployment: Identify who is authorized to officially approve the deployment and use of a technology, and the conditions necessary for deployment and use, if applicable.
    c. Training: Require training, and perhaps certification or other documented proficiency, if applicable, of all personnel who will be managing, maintaining, and/or using a technology. Training should also cover privacy protections on the use of the technology, and the impact and sanctions for potential violations.
    d. Operational Use: Identify specific operational factors that must be addressed in deployment and use of a technology. (For example, for ALPR, the officer should i) verify that the system has correctly "read" the license plate characters; ii) verify the state of issue of the license plate; iii) verify that the "hot list" record that triggered the alert is still active in the state or NCIC stolen vehicle or other file, and confirm the

hit with the entering agency; and iv) recognize that the driver of the vehicle may not be the registered owner).

e. Recordkeeping: Require recordkeeping practices that document all deployments of the technology, including who authorized the deployment; how, when, and where the technology was deployed; results of deployments; and any exceptions. Recordkeeping will support efforts to properly manage technology implementation, ensure compliance with agency policies, enable transparency of operations, enable appropriate auditing review, and help document business benefits realization.

6. Data Collection, Access, Use, and Retention
    a. Collection: Define what data will be collected, how data will be collected, the frequency of collection, how and where data will be stored, and under what authority and conditions the data may be purged, destroyed, or deleted in compliance with applicable local, state, and/or federal recordkeeping statutes and policies, court orders, etc. Identify the destruction/deletion methods to be used.
    b. Access and Use: Define what constitutes authorized use of data captured, stored, generated, or otherwise produced by a technology. Define who is authorized to approve access and use of the data, for what purposes and under what circumstances.
    c. Information Sharing: Specify whether data captured, stored, generated, or otherwise produced by a technology can be shared with other agencies, under what circumstances, how authorization is provided, how information that is shared is tracked/logged, how use is monitored, and how policy provisions (including privacy) will be managed and enforced. Any agency contributing and/or accessing shared information should be a signatory of a data sharing Memorandum of Understanding (MOU). Dissemination of any shared information should be governed by compliance with applicable state and federal laws, standards, agency privacy policies, and procedures as agreed in the MOU.
    d. Security: Define information systems security requirements of the technology and access to the data to ensure the integrity of the systems and confidentiality of the data. The security policy should address all state and federal mandated security policies, and clearly address procedures to be followed in the event of a loss, compromise, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of data, including how and when affected persons will be notified, and remedial and corrective actions to be taken.
    e. Data Retention and Use: Establish data retention schedules in accordance with state or federal law or policy, access privileges, purge,

and deletion criteria for all data captured, stored, generated, or otherwise produced by a technology. Agencies should consider differentiating between data that are part of an ongoing or continuing investigation and information that is gathered and retained without specific suspicion or direct investigative focus. Agencies may wish to limit the retention of general surveillance data. Empirical research assessing the performance of a technology may assist in determining an appropriate retention schedule.

7. Oversight, Evaluation, Auditing, and Enforcement
    a. Oversight: Establish a reporting mechanism and a protocol to regularly monitor the use and deployment of a technology to ensure strategic alignment and assessment of policy compliance.
    b. Evaluation: Regularly assess the overall performance of a technology so that it can i) identify whether a technology is performing effectively, ii) identify operational factors that may impact performance effectiveness and/or efficiency, iii) identify data quality issues, iv) assess the business value and calculate return on investment of a technology, and v) ensure proper technology refresh planning.
    c. Auditing: Audit all access to data captured, stored, generated, or otherwise produced by a technology to ensure that only authorized users are accessing the data for legitimate and authorized purposes, and establish regular audit schedules.
    d. Enforcement: Establish procedures for enforcement if users are suspected of being or have been found to be in noncompliance with agency policies.

Conclusion

Realizing the value that technology promises law enforcement can only be achieved through proper planning, implementation, training, deployment, use, and management of the technology and the information it provides. Like all resources and tools available to law enforcement, the use of new technologies must be carefully considered and managed. Agencies must clearly articulate their strategic goals for the technology, and this should be aligned with the broader strategic plans of the agency and safety needs of the public. Thorough and ongoing training is required to ensure that the technology performs effectively, and that users are well versed in the operational policies and procedures defined and enforced by the agency. Policies must be developed and strictly enforced to ensure the quality of the data, the security of the system, compliance with applicable laws and regulations, and the privacy of information gathered. Building robust auditing requirements into agency policies will help enforce proper use of the system, and reassure the public that their privacy interests are recognized and protected. The development of these policies is a proven way for executives to ensure they are taking full advantage of technology to assist in providing the best criminal justice services, while protecting the privacy, civil rights, and civil liberties of citizens.

[1] This Technology Policy Framework was developed by an ad-hoc committee of law enforcement executives and subject matter experts representing IACP Divisions, Committees, Sections, the IACP National Law Enforcement Policy Center, and other organizations and groups, including the Criminal Intelligence Coordinating Council, Major Cities Chiefs Association, National Sheriffs' Association, Major County Sheriffs' Association, Association of State Criminal Investigative Agencies, the Institute for Intergovernmental Research (IIR), the Integrated Justice Information Systems (IJIS) Institute, and federal partners.

[2] The American Civil Liberties Union (ACLU) recently released two reports addressing law enforcement technologies—ALPR and body-worn video. Both reports discuss the value of the technology to law enforcement operations and investigations, and both call for policies addressing deployment, operations, data retention, access, and sharing. Catherine Crump, *You are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements,* (New York: ACLU, July 2013), at https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record, and Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, a Win for All,* (New York: ACLU, October 2013), at https://www.aclu.org/technology-and-liberty/police-body-mounted-cameras-right-policies-place-win-all. *Also see,* Massachusetts Senate Bill S.1648, *An Act to Regulate the Use of Automatic License Plate Reader Systems,* Cynthia S. Creem, Sponsor, at https://malegislature.gov/Bills/188/Senate/S1648; Cynthia Stone Creem and Jonathan Hecht, "Check it, then chuck it," *The Boston Globe,* December 20, 2013, at http://www.bostonglobe.com/opinion/2013/12/20/podium-license/R1tKQerV0YAPLW6VCKodGK/story.html; Shawn Musgrave, "Boston Police halt license scanning program," *The Boston Globe,* December 14, 2013, at http://www.bostonglobe.com/metro/2013/12/14/boston-police-suspend-use-high-tech-licence-plate-readers-amid-privacy-concerns/B2hy9UIzC7KzebnGyQ0JNM/story.html; Ashley Luthern and Kevin Crowe, "Proposed Wisconsin bill would set rules for license-plate readers," *Milwaukee Journal Sentinel*, December 3, 2013, at http://www.jsonline.com/news/milwaukee/proposed-wisconsin-bill-would-set-rules-for-license-plate-readers-b99155494z1-234324371.html; Dash Coleman, "Tybee Island abandons license plate scanner plans," *Savannah Morning News,* December 3, 2013, at http://savannahnow.com/news/2013-12-02/tybee-island-abandons-license-plate-scanner-plans#.UqCAy8RDuN0; Kristian Foden-Vencil, "Portland police are collecting thousands of license plate numbers every day," *Portland Tribune*, December 3, 2013, at http://portlandtribune.com/pt/9-news/203130-portland-police-are-collecting-thousands-of-license-plate-numbers-every-day; Alicia Petska, "City Council split over how to handle license plate reader concerns," *The News & Advance,* (Lynchburg, VA), November 12, 2013, at http://www.newsadvance.com/news/local/article_5327dc78-4c18-11e3-bc28-001a4bcf6878.html; Jonathan Oosting, "Proposal would regulate license plate readers in Michigan, limit data stored by police agencies," *MLive,* (Lansing, MI), September 9, 2013, at http://www.mlive.com/politics/index.ssf/2013/09/proposal_would_regulate_licens.html; Katrina Lamansky, "Iowa City moves to ban traffic cameras, drones, and license plate recognition," *WQAD*, June 5, 2013, at http://wqad.com/2013/06/05/iowa-city-moves-to-ban-traffic-cameras-drones-and-license-plate-recognition/; Richard M. Thompson, II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses,* (Washington, DC: Congressional Research Service, April 3, 2013), at http://www.fas.org/sgp/crs/natsec/R42701.pdf; Somini Sengupta, "Rise of Drones in U.S. Drives

Efforts to Limit Police Use," *New York Times,* February 15, 2013, at http://www.nytimes.com/2013/02/16/technology/rise-of-drones-in-us-spurs-efforts-to-limit-uses.html?pagewanted=all; Stephanie K. Pell and Christopher Soghoian, "Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact," *Berkeley Technology Law Journal,* Vol. 27, No. 1, pp. 117-196, (2012), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1845644; and Stephen Rushin, "The Legislative Response to Mass Police Surveillance," 79 *Brooklyn Law Review* 1*,* (2013), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344805. All accessed December 30, 2013.

[3] Personally identifiable information (PII) has been defined as "…any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." Government Accountability Office (GAO), *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, (Washington, D.C.: GAO, May 2008), p. 1, at http://www.gao.gov/new.items/d08536.pdf. McCallister, *et. al.,* define "linked" information as "information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual." Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology,* (Gaithersburg, MD: NIST, April 2010), p. 2-1, at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. McCallister, *et. al.,* go on to describe *linked* and *linkable* information: "For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable." *Id.* Both accessed December 30, 2013.

[4] Justice Harlan first articulated a "constitutionally protected reasonable expectation of privacy" in *Katz v. United States*, 389 U.S. 347 (1967), at 361. Justice Harlan's two-fold test is "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* Many of the technologies being deployed by law enforcement capture information that is publicly exposed, such as digital photographs and video of people and vehicles, or vehicle license plates in public venues (i.e., on public streets, roadways, highways, and public parking lots), and there is little expectation of privacy. "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *United States v. Knotts*, 460 U.S. 276 (1983), at 281. Law enforcement is free to observe and even record information regarding a person's or a vehicle's movements in public venues. The U.S. Supreme Court, however, has ruled that the electronic compilation of otherwise publicly available but

difficult to obtain records alters the privacy interest implicated by disclosure of that compilation. *U.S. Department of Justice v. Reporters Committee for Freedom of the Press,* 489 U.S. 749 (1989). Automation overwhelms what the Court referred to as the *practical obscurity* associated with manually collecting and concatenating the individual public records associated with a particular person into a comprehensive, longitudinal criminal history record. "…[T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." *Id.,* at p. 764. This has subsequently been referred to as the "mosaic theory" of the Fourth Amendment. *United States v. Maynard,* 615 F.3d 544 (D.C. Cir.) (2010). *See also,* Orin Kerr, "The Mosaic Theory of the Fourth Amendment," *Michigan Law Review*, Vol. 111, p. 311, (2012), at http://www.michiganlawreview.org/assets/pdfs/111/3/Kerr.pdf. Accessed December 30, 2013.

[5] These universal principles largely align with the Fair Information Practices (FIPs) first articulated in 1973 by the Department of Health, Education & Welfare (HEW). HEW, *Records, Computers and the Rights of Citizens*, July 1973, at http://epic.org/privacy/hew1973report/default.html. *See,* Robert Gellman, *Fair Information Practices: A Basic History,* Version 2.02, November 11, 2013, at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf. Comparable principles have been articulated by various governmental agencies, including the U.S. Department of Homeland Security, (Hugo Teufel, III, *Privacy Policy Guidance Memorandum, Number: 2008-01,* (Washington, DC: DHS, December 29, 2008), pp. 3-4, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf); the Home Office in the United Kingdom (Home Office, *Surveillance Camera Code of Practice,* (London, UK; The Stationery Office, June 2013), pp 10-11, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf); and the Information and Privacy Commissioner of Ontario, Canada (Ann Cavoukian, *Guidelines for the Use of Video Surveillance Cameras in Public Places,* (Ontario, Canada: Information and Privacy Commissioner of Ontario, September 2007), pp. 5-6, at: http://www.ipc.on.ca/images/Resources/up-3video_e_sep07.pdf, and Ann Cavoukian, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigative Report (Privacy Investigation Report MC07-68)*, (Ontario, Canada: Information and Privacy Commissioner of Ontario, March 3, 2008), p 3, at: http://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf). *Also see*, National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment,* (The National Academies Press: Washington, D.C., 2008), at http://nap.edu/catalog.php?record_id=12452. All accessed December 30, 2013.

[6] Law enforcement is not, for example, expected to notify the subjects of lawfully authorized wiretaps that their conversations are being monitored and/or recorded. These deployments, however, are typically subject to prior judicial review and authorization. *See, e.g., Katz v. United States,* 389 U.S. 347 (1967); *Berger v. New York,* 388 U.S. 41 (1967); *Title III, Omnibus Crime Control and Safe Streets Act of 1968*, 18 U.S.C. §§ 2510-2522, as amended by the *Electronic Communications Privacy Act of 1986*.

[7] Federal Bureau of Investigation, *Criminal Justice Information Services (CJIS) Security Policy,* Version 5.2, August 9, 2013, CJISD-ITS-DOC-08140-5.2, at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view. Accessed December 30, 2013.

[8] Additional guidance regarding safeguarding personally identifiable information can be found in the Office of Management and Budget (OMB) Data Breach notification policy (M-07-16), at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf, and state data breach notification laws available from the National Conference of State Legislatures, at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Accessed December 30, 2013.

[9] *See, e.g.,* International Association of Chiefs of Police, *Model Policy: License Plate Readers*, August 2010 http://iacppolice.ebiz.uapps.net/personifyebusiness/OnlineStore/ProductDetail/tabid/55/Default.aspx?ProductId=1223; Paula T. Dow, Attorney General, *Directive No. 2010-5, Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data,* (Trenton, NJ: Office of the Attorney General, December 3, 2010), at http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf; Office of the Police Ombudsman, *2011 Annual Report: Attachment G: Body-Worn Video & Law Enforcement: An Overview of the Common Concerns Associated with Its Use*, (Spokane, WA: Spokane Police Ombudsman, February 20, 2012), at http://www.spdombudsman.com/wp-content/uploads/2012/02/Attachment-G-Body-Camera-Report.pdf; ACLU, *Model Policy: Mobile License Plate Reader (LPR) System,* (Des Moines, IA: ACLU, September 19, 2012), at http://www.aclu-ia.org/iowa/wp-content/uploads/2012/09/Model-ALPR-Policy-for-Iowa-Law-Enforcement.pdf. Many of these policy elements are also addressed in the National Research Council's report, *op. cit.,* specifically in chapter 2, "A Framework for Evaluating Information-Based Programs to Fight Terrorism or Serve Other Important National Goals," at pp. 44-67. All accessed December 30, 2013

[10] A privacy impact assessment (PIA) is "a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme." Roger Clarke, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review,* 25, 2 (April 2009), pp. 125-135, at http://www.rogerclarke.com/DV/PIAHist-08.html. Law enforcement agencies should consider using the Global Advisory Committee's *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities* at https://it.ojp.gov/gist/47/Guide-to-Conducting-Privacy-Impact-Assessments-for-State--Local--and-Tribal-Justice-Entities. This resource leads policy developers through appropriate privacy risk assessment questions that evaluate the process through which PII is collected, stored, protected, shared, and managed by an electronic information system or online collection application. The IACP published *Privacy Impact Assessment Report for the Utilization of License Plate Readers,* (Alexandria, VA: IACP, September 2009), at http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf. For a list of PIAs completed by the U.S. Department of Justice, *see* http://www.justice.gov/opcl/pia.htm; Department of Homeland Security, *see* https://www.dhs.gov/privacy-office-privacy-impact-assessments-pia. All accessed December 30, 2013.

Filed 5/6/15

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION THREE

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SOUTHERN CALIFORNIA et al., Petitioners, v. THE SUPERIOR COURT OF LOS ANGELES COUNTY, Respondent; COUNTY OF LOS ANGELES et al., Real Parties in Interest.	B259392 (Los Angeles County Super. Ct. No. BS143004)

PETITION for Writ of Mandate from an order of the Superior Court of Los Angeles County, James C. Chalfant, Judge. Petition denied.

Peter Bibring for Petitioner American Civil Liberties Union Foundation of Southern California.

Jennifer Lynch for Petitioner Electronic Frontier Foundation.

No Appearance for Respondent.

Michael N. Feuer, City Attorney, Carlos De La Guerra, Managing Assistant City Attorney, Debra L. Gonzales, Assistant City Attorney, and Heather L. Aubry, Deputy City Attorney, for Real Parties in Interest City of Los Angeles and the Los Angeles Police Department.

Collins Collins Muir + Stewart, Eric Brown, Tomas A. Guterres and James C. Jardin for Real Parties in Interest County of Los Angeles and the Los Angeles Sheriff's Department.

INTRODUCTION

In this writ proceeding we must determine whether the California Public Records Act (CPRA) exemption for law enforcement records of investigations (Gov. Code, § 6254, subd. (f))[1] applies to records generated by a system of high-speed cameras that automatically scan and catalogue license plate images to aid law enforcement in locating vehicles associated with a suspected crime. We conclude the exemption applies.

For more than a decade, the Los Angeles Police Department (LAPD) and Los Angeles Sheriff's Department (LASD), agencies of Real Parties in Interest the City and County of Los Angeles (collectively, Real Parties), have used Automatic License Plate Reader (ALPR) technology to automate a process that officers ordinarily perform manually—checking license plates to determine whether a vehicle is stolen or otherwise wanted in connection with a crime. Real Parties' ALPR systems consist of specialized cameras mounted to patrol cars or stationary structures that scan license plates in their immediate vicinity and record the license plate number together with the time and location of the scan. At virtually the same time, the ALPR system checks every license plate number it scans against a list of known license plates associated with suspected crimes—a so-called "hot list." If the system registers a hit, patrol officers are immediately notified that a hot list vehicle is in their vicinity. Regardless of whether there is a hit, the system records the plate scan data, which Real Parties retain for up to five years for use in future investigations.

---

[1] Subsequent statutory references are to the Government Code, unless otherwise designated.

Petitioners American Civil Liberties Union Foundation of Southern California and Electronic Frontier Foundation sent Real Parties a CPRA request for their policies and guidelines concerning use of ALPR technology, as well as all ALPR plate scan data Real Parties collected during a single week in August 2012. Real Parties agreed to produce the policies and guidelines, but refused to disclose the week's worth of ALPR data, citing the law enforcement investigative records exemption and privacy concerns. Petitioners filed a petition for writ of mandate seeking to compel production of the ALPR data under the CPRA. The trial court denied the petition, concluding the records are exempt as records of law enforcement investigations under section 6254, subdivision (f). Guided by Supreme Court precedent extending the exemption to "records of investigations conducted for the purpose of uncovering information surrounding the commission of the violation [of law] and its agency" (*Haynie v. Superior Court* (2001) 26 Cal.4th 1061, 1071 (*Haynie*)), we likewise conclude the exemption applies to records generated by the ALPR system in the course of scanning license plates to locate automobiles associated with a suspected crime under investigation. Accordingly, we deny the writ petition.

FACTS AND PROCEDURAL BACKGROUND

The relevant facts are not in dispute. Real Parties each maintain an ALPR system that consists of several high-speed cameras mounted on fixed structures and patrol cars that automatically capture an image of every passing vehicle's license plate in their immediate vicinity. The system uses "character recognition software" to read the license plate's number from the image and "almost instantly" checks the number against a list of "known license plates" associated with suspected crimes—or a "hot list"—to determine whether a vehicle may be stolen or otherwise associated with a crime, AMBER alert or outstanding warrant. If a mobile ALPR unit detects a license plate on the hot list, officers are notified of the "hit" by an audible alert and notation on their patrol car's computer screen. ALPR fixed positions similarly notify a central dispatch unit when a hit is detected.

In addition to extracting the license plate number, the ALPR system records the date and location where it captured the plate's image. The system transmits this "plate scan data" to an ALPR server within Real Parties' confidential computer networks. LAPD estimates it records plate scan data for approximately 1.2 million cars per week; LASD estimates that figure to be between 1.7 and 1.8 million plate scans for its ALPR system. LAPD retains plate scan data for five years under its current policy. LASD retains the data for two years, although it would prefer to retain the data indefinitely.

In addition to receiving immediate notification from the ALPR system when it locates a license plate on the hot list, Real Parties can also query stored plate scan data to assist in subsequent law enforcement investigations. For instance, LAPD investigators have used stored ALPR data to identify a vehicle that was present at an armed robbery and, in another instance, a vehicle directly linked to a homicide. Real Parties maintain policies restricting access to plate scan data for law enforcement purposes only.

On August 30 and September 4, 2012, Petitioners sent substantially identical CPRA requests to LAPD and LASD seeking records related to those agencies' use of ALPR technology, including "all ALPR data collected or generated" during a one-week period in August 2012, consisting of, "at a minimum, the license plate number, date, time, and location information for each license plate recorded." The CPRA request also sought "any policies, guidelines, training manuals and/or instructions on the use of ALPR technology and the use and retention of ALPR data, including records on where the data is stored, how long it is stored, who has access to the data, and how they access the data."

Real Parties each agreed to produce records responsive to Petitioners' requests for policies, guidelines and training manuals concerning the use, access, and retention of ALPR plate scan data. Real Parties refused to produce the requested week's worth of plate scan data, however, citing, among other things, the exemption for records of law enforcement investigations.

On May 6, 2013, Petitioners filed a verified petition for writ of mandate to compel production of the ALPR plate scan data under the CPRA.

Real Parties each opposed the petition, again citing the exemption for records of law enforcement investigations under section 6254, subdivision (f), as well as the "catchall" exemption under section 6255.[2] With their opposition briefs, Real Parties filed supporting declarations by their subject matter experts detailing the technical aspects of their respective ALPR systems and the ways each law enforcement agency uses the technology in practice.

On August 21, 2014, the court held a trial on Petitioners' writ petition. On August 27, 2014, the court entered an order affirming Real Parties' decision to withhold the ALPR plate scan data, concluding the data was subject to the records of investigations exemption under section 6254, subdivision (f) and the catchall exemption under section 6255.

DISCUSSION

1. *Standard of Review*

A trial court order under the CPRA, either directing disclosure by a public official or affirming the public official's decision to refuse disclosure, is immediately reviewable by petition to the appellate court for issuance of an extraordinary writ. (§ 6259, subd. (c).) "The standard for review of the order is 'an independent review of the trial court's ruling; factual findings made by the trial court will be upheld if based on substantial evidence.' " (*City of San Jose v. Superior Court* (1999) 74 Cal.App.4th 1008, 1016.) The interpretation of the CPRA, and application of the statute to undisputed facts is a question of law subject to de novo review. (*Lorig v. Medical Board* (2000) 78 Cal.App.4th 462, 467.)

[2] Under section 6255, a public agency may justify withholding records otherwise subject to CPRA disclosure requirements by demonstrating that "on the facts of the particular case the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record."

2. *The Records of Investigations Exemption Under Government Code Section 6254, Subdivision (f)*

The CPRA declares that "access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state." (§ 6250.) The statute's explicit purpose is to increase freedom of information by giving the public access to information in the public agencies' possession. (*CBS, Inc. v. Block* (1986) 42 Cal.3d 646, 651.) "Maximum disclosure of the conduct of governmental operations was to be promoted by the [CPRA]." (*Id.* at pp. 651-652.) To that end, the CPRA provides that "every person has a right to inspect any public record, except as hereafter provided." (§ 6253, subd. (a).) Hence, "all public records are subject to disclosure unless the Legislature has expressly provided to the contrary." (*Williams v. Superior Court* (1993) 5 Cal.4th 337, 346 (*Williams*); *Haynie, supra,* 26 Cal.4th at p. 1068.) Consistent with the CPRA's purpose, "[s]tatutory exemptions from compelled disclosure are narrowly construed." (*California State University, Fresno Assn., Inc. v. Superior Court* (2001) 90 Cal.App.4th 810, 831.)

Real Parties contend, and the trial court found, that the plate scan records generated by the ALPR system constitute records of investigations which are exempt from disclosure under section 6254, subdivision (f). In pertinent part, subdivision (f) authorizes a public agency to withhold "[r]ecords of . . . investigations conducted by . . . any state or local police agency, or any investigatory or security files compiled by any other state or local police agency . . . ." While broadly shielding the records themselves from disclosure, the CPRA requires law enforcement agencies to disclose certain information derived from the records, as provided in subdivisions (f)(1) and (f)(2).[3]

---

[3] Notwithstanding the general directive to narrowly construe such exemptions, our Supreme Court has explained that section 6254, subdivision (f) "articulates a *broad exemption* from disclosure for law enforcement investigatory records," which is limited only by requirements in subdivisions (f)(1) and (f)(2) to "provide *certain information derived from the records* about the incidents under investigation." (*Williams, supra,* 5 Cal.4th at p. 349, italics added.) That is, "[i]nstead of adopting criteria that would require the exemption's applicability to be determined on a case-by-case basis," the

(*Williams, supra,* 5 Cal.4th at p. 353; *Haynie, supra,* 26 Cal.4th at p. 1068.) The parties agree that the derivative categories of information to be disclosed under these subsections—information about arrests and arrestees (§ 6254, subd. (f)(1)) and complaints and requests for assistance (§ 6254, subd. (f)(2))—are not at issue in this case.

What is at issue is the meaning of the term "investigations" in section 6254, subdivision (f), and whether the functions performed by the ALPR system can properly be characterized as investigations under the statute. Though the CPRA does not define the term, and no case has considered whether records generated by an automated process, like that performed by the ALPR system, qualify for exemption under subdivision (f), our Supreme Court has articulated some general principles to guide our analysis.

First, the exemption for records of investigation encompasses routine investigations undertaken to determine if a violation of law has, or may have, occurred. In rejecting an interpretation that would exclude such records from the exemption's purview, the Supreme Court in *Haynie* explained, "The Court of Appeal, in ordering disclosure, reasoned that the citizen report . . . did not 'necessarily' describe a crime and that the [law enforcement action] was a 'routine police inquiry' based on mere suspicion of criminal conduct. *These factors are of no significance under the statute*. In exempting '[r]ecords of complaints to, or investigations conducted by' law enforcement agencies, section 6254(f) *does not distinguish between investigations to determine if a crime has been or is about to be committed and those that are undertaken once criminal conduct is apparent*."[4] (*Haynie, supra,* 26 Cal.4th at p. 1070, fn. 6, italics added.)

Legislature "limited the CPRA's exemption for law enforcement investigatory files . . . [by] adopt[ing] a series of amendments that required the disclosure of *information derived from the records* while, in most cases, preserving the exemption for the records themselves." (*Id.* at p. 353.)

[4] This distinguishes the records of investigations from "investigatory . . . *files* compiled by any . . . local agency for correctional, law enforcement, or licensing purposes. . . ." (§ 6254, subd. (f), italics added.) As the Supreme Court explained in *Williams*, it is "well established that 'information in public files [becomes] exempt as "investigatory" material only when the prospect of enforcement proceedings [becomes] concrete and definite.' " (*Williams, supra*, 5 Cal.4th at p. 356.) "Such a qualification is

Second, while routine investigations are within the exemption's ambit, not everything that law enforcement does is shielded from disclosure. As the court explained in *Haynie*, "[o]ften, officers make inquiries of citizens for purposes related to crime prevention and public safety that are *unrelated* to either civil or criminal investigations. The records of investigation exempted under section 6254(f) encompass only those *investigations undertaken for the purpose of determining whether a violation of law may occur or has occurred*. If a violation or potential violation is detected, *the exemption also extends to records of investigations conducted for the purpose of uncovering information surrounding the commission of the violation and its agency*." (*Haynie, supra,* 26 Cal.4th at p. 1071, italics added.)

Third, the exemption shielding records of investigations from disclosure does not lapse when the investigation that prompted the records' creation ends. As the high court stated in *Williams* with respect to the exemption for investigatory files, "It is noteworthy that nothing [in the statute's language] purports to place a time limit on the exemption for investigatory files. Indeed, a file 'compiled by . . . [a] police agency' or a file 'compiled by any other state or local agency for . . . law enforcement . . . purposes' continues to meet that definition after the investigation has concluded. If the Legislature had wished to limit the exemption to files that were 'related to pending investigations,' words to achieve that result were available. It is not the province of courts 'to insert what has been omitted.' " (*Williams, supra,* 5 Cal.4th at p. 357.) The same is true for records of investigations—they continue to be "[r]ecords of . . . investigations conducted by . . . any

---

necessary to prevent an agency from attempting to 'shield a record from public disclosure, *regardless of its nature*, simply by placing it in a file labelled "investigatory." ' " (*Haynie, supra,* 26 Cal.4th at p. 1069, quoting *Williams,* at p. 355.) However, the " 'concrete and definite' qualification to the exemption in section 6254(f) 'relates only to information which is not itself exempt from compelled disclosure, but claims exemption only as part of an investigatory file. Information independently exempt, such as "intelligence information" [or records of investigations at issue in *Haynie*], is not subject to the requirement that it relate to a concrete and definite prospect of enforcement proceedings.' " (*Haynie,* at p. 1069, quoting *American Civil Liberties Union Foundation v. Deukmejian* (1982) 32 Cal.3d 440, 449, fn. 10.)

state or local police agency" even after the investigation that prompted their creation ends. (§ 6254, subd. (f).)

Finally, as alluded to in the foregoing quotation from *Williams*, the Supreme Court has cautioned against courts placing nonstatutory limitations on the scope of section 6254, subdivision (f). As the court elaborated in *Williams*, referring to the required disclosures under section 6254, subdivisions (f)(1) and (f)(2), "These provisions for mandatory disclosure from law enforcement investigatory files represent the Legislature's judgment, set out in exceptionally careful detail, about what items of information should be disclosed and to whom. Unless that judgment runs afoul of the Constitution it is not our province to declare that the statutorily required disclosures are inadequate or that the statutory exemption from disclosure is too broad. . . . Requests for broader disclosure must be directed to the Legislature." (*Williams, supra,* 5 Cal.4th at p. 361.)

With these principles in mind, we turn to whether the plate scan data generated by the ALPR system constitute records of investigation under section 6254, subdivision (f).

3. *Plate Scan Data Generated by the ALPR System Are Records of Investigations Exempt from Disclosure Under Government Code Section 6254, Subdivision (f)*

Drawing on the guidance from *Haynie* and *Williams*, Real Parties contend the plate scans performed by the ALPR system are "investigations" within the meaning of section 6254, subdivision (f) because they are "conducted for the purpose of uncovering information surrounding the commission of the violation [of law] and its agency." (*Haynie, supra,* 26 Cal.4th at p. 1071.) Citing the declaration by LAPD's subject matter expert, Real Parties stress that the ALPR system uses "character recognition software" to read license plate numbers and "almost instantly" checks those numbers against a list of "known license plate[s]" associated with suspected crimes to "determine whether a vehicle may be stolen or otherwise associated with a crime." The LASD's declarant described the ALPR system's function in similar terms, explaining that by utilizing the system to "automatically" check license plate scans against a "hot list" of plates

associated with suspected crimes, "[t]he [LASD] uses ALPR technology to investigate specific crimes that involve motor vehicles, including but not limited to stolen motor vehicles, Amber alerts that identify a specific motor vehicle, warrants that relate to the owner of a specific motor vehicle, and license plates of interest that relate to a specific investigation being conducted by [LASD] investigatory personnel." Thus, Real Parties contend the license plate scan and almost instantaneous check against the hot list constitutes an investigation under section 6254, subdivision (f), because the ALPR system is attempting to detect and uncover criminal activity. (*Haynie*, at p. 1071.)

Expanding on the foregoing analysis, Real Parties argue the records generated by the ALPR system in performing the scans and hot list checks are records of investigations and, therefore, exempt from disclosure under section 6254, subdivision (f). As counsel for the LASD put it at the trial below, plate scan data generated by the ALPR system is necessarily a record of an investigation because "[t]hese records would not exist were the County or the City not investigating specific crimes in an attempt to locate persons who are suspected of having committed crimes." We agree. In the *Haynie* court's words, these records exist only because Real Parties are trying to "uncover[ ] information surrounding the commission of [a] violation [of law] and its agency." (*Haynie, supra,* 26 Cal.4th at p. 1071.) As evidenced by the LAPD and LASD declarations, Real Parties have deployed the ALPR system to assist in law enforcement investigations involving an identified automobile's license plate number. It follows that the records the ALPR system generates in the course of attempting to detect and locate these automobiles are records of those investigations. The exemption under section 6254, subdivision (f) broadly shields these records from disclosure, subject to requirements pertaining to derivative information (see § 6254, subds. (f)(1) & (f)(2)) not at issue here. (See *Williams, supra,* 5 Cal.4th at pp. 353, 361; *Haynie,* at p. 1068.)

Petitioners argue the ALPR plate scans are not investigations within the exemption's purview. Unlike the cases that have applied the exemption, which all "involve[d] requests for documents related to *targeted investigations of specific criminal acts*" (italics added), Petitioners argue the plate scans conducted by ALPR systems "are

not precipitated by any specific criminal investigation." Rather, Petitioners assert, ALPR systems "photograph every license plate that comes into view . . . regardless of whether the car or its driver is linked to criminal activity." They contend, ALPR systems "do not conduct investigations; they collect data." We disagree.

Contrary to Petitioners' premise, the plate scans performed by the ALPR system are precipitated by specific criminal investigations—namely, the investigations that produced the "hot list" of license plate numbers associated with suspected crimes. As Real Parties' experts both testified, the ALPR system's principal purpose is to check license plates against the hot list to determine whether a vehicle is connected to a crime under investigation. In this way, the ALPR system replicates, albeit on a vastly larger scale, a type of investigation that officers routinely perform manually by visually reading a license plate and entering the plate number into a computer to determine whether a subject vehicle might be stolen or otherwise associated with a crime.[5] The fact that the ALPR system automates this process does not make it any less an investigation to locate automobiles associated with specific suspected crimes.

Nor does the fact that the ALPR system scans every license plate within view, "regardless of whether the car or its driver is linked to criminal activity," mean the system is not performing an investigation. As explained in *Haynie*, "[i]n exempting '[r]ecords of . . . investigations conducted by' law enforcement agencies, section 6254(f) *does not distinguish between investigations to determine if a crime has been or is about to be committed and those that are undertaken once criminal conduct is apparent*."

---

[5] Petitioners suggest the "collection of plate data"—i.e., the photographing and scanning of a license plate—can be separated from "its later investigative uses"—i.e., the near instantaneous check against the hot list. This argument ignores that the plate scan is an integral part of the ALPR system's process for locating automobiles on the hot list. Just as an officer cannot investigate whether an automobile has been associated with a suspected crime without visually observing and reading its license plate number, so too the ALPR system cannot determine whether a license plate number is on the hot list without scanning the plate. The collection of plate data and hot list check are part and parcel of the same investigative process—without the plate scan there can be no investigation.

(*Haynie, supra,* 26 Cal.4th at p. 1070, fn. 6, italics added.) Contrary to Petitioners' implicit contention, our Supreme Court has repeatedly rejected the notion that a "concrete and definite" prospect of enforcement must be shown to exempt records of investigations from disclosure. (*Id.* at pp. 1069-1071; see also *Williams, supra,* 5 Cal.4th at pp. 354-356.) The ALPR system necessarily scans every car in view, just as human officers would in attempting to identify a stolen vehicle. The fact that non-hot list vehicles are necessarily checked does not mean there was no investigation. (See fn. 6, *post*.)

Lastly, Petitioners emphasize the volume and retention of plate scan data to highlight the differences between ALPR scans and more traditional investigative techniques. In Petitioners' view, because Real Parties' ALPR systems each generate more than a million system-wide scans each week, and retain data from these scans for two to five years, they "do not conduct investigations; they collect data."

There are two problems with this argument. We have already discussed the first—the ALPR systems are not merely recording data; rather, Real Parties have deployed these systems primarily to detect and locate vehicles that have been connected to a suspected crime. The fact that ALPR technology generates substantially more records than an officer could generate in manually performing the same task does not mean the ALPR plate scans are not records of investigations.[6]

---

[6] For instance, setting practical considerations aside, Real Parties could hypothetically deploy human patrol units to photograph every license plate they pass during a specific period on a specific route in order to later compare those photographs against a hot list of license plates associated with suspected crimes. Though this tactic would generate a massive number of license plate photographs, of which very few could be expected to appear on the hot list, no one could claim these photographs, and the associated time and location data logged by the officers, were not records of the investigations these officers performed. The fact that the ALPR system automates this process and generates exponentially more records than officers could humanly produce has no bearing on whether those plate scans and associated data are records of investigations under section 6254, subdivision (f).

Second, though ALPR data is retained for two to five years after the initial hot list check, this does not strip an investigative record of its exempt status under section 6254, subdivision (f). As our Supreme Court explained in *Williams*, "nothing [in the statute's language] purports to place a time limit on the exemption for investigative files." (*Williams, supra,* 5 Cal.4th at p. 357.) Records generated by the ALPR system for the purpose of locating automobiles associated with a suspected crime, like the investigative files discussed in *Williams*, continue to meet the applicable statutory definition even after the investigations for which they were created conclude—that is, they continue to be "[r]ecords of . . . investigations conducted by . . . any state or local police agency." (§ 6254, subd. (f); see *Williams*, at p. 357.) Thus, for our purposes in interpreting the exemption, it is of no moment that Real Parties retain the records in a database for years after the initial hot list check.

To be sure, the automated nature of the ALPR system, with its capacity to capture and record millions of plate scans throughout Los Angeles City and County, sets it apart from the traditional investigatory techniques that courts have considered in earlier cases addressing the scope of the investigative records exemption. But that distinction is irrelevant to the question of whether the ALPR system's core function is to "uncover[ ] information surrounding the commission of the violation [of law] and its agency"—i.e., to investigate suspected crimes. (*Haynie, supra,* 26 Cal.4th at p. 1071.). We conclude that it is, and that the records generated in the course of performing that function are records of these investigations. The investigative records exemption applies and shields the plate scan data from disclosure under the CPRA.

Because we conclude the exemption under section 6254, subdivision (f) supports Real Parties' decision to withhold the ALPR plate scan data, we do not address whether Real Parties also met their burden under section 6255's catchall exemption.

DISPOSITION

The petition for writ of mandate is denied. Real Parties are entitled to recover their costs in this writ proceeding.

CERTIFIED FOR PUBLICATION

KITCHING, Acting P. J.

We concur:

ALDRICH, J.

EGERTON, J.*

* Judge of the Los Angeles Superior Court, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

Body-Worn Camera System

447.1 PURPOSE

Purpose

(a) To provide policy and procedures for the use of the body-worn camera system which includes video recording of field activity in the course of official police duties.

(b) The use of the body-worn camera system provides documentary evidence for criminal investigations, internal or administrative investigations, and civil litigation. Personnel shall utilize this device in accordance with the provisions in this policy to maximize the effectiveness of the audio/video documentation, to achieve operational objectives, and to ensure evidence integrity.

447.2 DEFINITIONS

(a) PERSONNEL - Personnel who are trained and assigned to use the body-worn camera system.

(b) ROUTINE - During the regular course of one's duties.

(c) BODY-WORN CAMERA SYSTEM DEVICE - The system is a body-worn, on-officer video camera.

447.3 RESPONSIBILITIES

(a) System Administrators - City of Fremont Info Systems and ITS personnel are designated Systems Adminstrators. Their duties include:

1. Operation and user administration of the system including software upgrades and system configuration changes
2. System evaluation and quality control

(b) Department Administrators - Department Administrators are designated by the Chief of Police. Their duties include:

1. Training
2. Policy and procedure review and evaluation
3. Coordination with IT regarding system related issues
4. Ensuring body-worn camera system files of evidentiary value are secured and maintained for a minimum of three (3) years. Ensure all other routine files are secured and maintained for three (3) years.
5. Ensuring body-worn camera system files are reviewed and released in accordance with federal, state, local statutes and the City of Fremont Police Department retention policy.

(c) Supervisors:

Adoption Date: 2015/05/19

1. Supervisors will ensure personnel utilize the body-worn camera system according to policy guidelines.
2. Supervisors may review all video files when there is a legitimate business purpose. Supervisors should review all files capturing use-of-force incidents, pursuits, and significant events.
3. Minor infractions (not criminal in nature) discovered during the routine review of recorded materials in accordance with departmental policy should be viewed as training opportunities and not as routine disciplinary actions. Should the behavior or action become habitual after being informally addressed, the appropriate disciplinary or corrective action shall be taken.
4. When reviewing the video files, supervisors who find an issue portrayed in the video that could be used for a training point will need the approval of the shift lieutenant and shall confer with the officer before showing the video file in briefing. The intent of showing the video files in the briefing setting is for training purposes only. Sergeants should work with the assigned training sergeant to look for opportunites to use the video files for departmental training purposes.

(d) Personnel utilizing the body-worn camera system shall:

1. Wear the device during any primary regular duty shift, and primary duty overtime shift, and when the Chief of Police or designee deems it appropriate to wear. Personnel will use only the body-worn camera system issued and approved by the Department. The wearing of any other personal video recording device is not authorized.
2. Ensure the battery is fully charged and operating properly.
3. Immediately report malfunctioning, damaged, or missing equipment to their immediate supervisor and notify the System Administrator via HelpDesk email prior to the end of their shift.
4. If a police report, field interrogation card, or citation is used to document an incident, use of the body-worn camera system should be noted.
5. Once video is captured, officers should identify body-worn camera system files as follows:

    (a) By the end of each shift, personnel will initiate the upload process. They will review new video, classify their files appropriately with the assigned case number, citation number, or incident history number, or leave it unassigned. The review and tagging will be completed prior to the end of shift unless a hold-over is approved by a sergeant.

    (b) Enter a title which includes information to identify the file, such as crime code, suspect name, location, event, etc.

    (c) Select the appropriate category or catagories.

Adoption Date: 2015/05/19

(d) The information may be entered via hand held device, mobile device, or FPD computer work station before the end of the shift.

(e) If appropriate, personnel will mark the digital evidence box in ARS.

(f) In the event of an equipment malfunction in the field resulting in no video files being captured, personnel will notify his/her supervisor. If a police report is written documenting the incident, personnel should note in the report the fact that a malfunction occurred. If no police report is written documenting the incident, personnel should note in the CAD incident history the fact that a malfunction occured.

447.4 ACTIVATION OF THE BODY-WORN CAMERA SYSTEM

(a) There are many situations where the use of the body-worn camera system is appropriate. This policy is not intended to describe every possible circumstance. At no time are personnel required to jeopardize their safety in order to activate a body-worn camera system. However, the body-worn camera system should be activated in required situations as soon as practicable. The activation of the body-worn camera system is required in any of the following incidents:

1. All enforcement and investigative contacts including: detentions and field interview (FI) situations, probation and parole searches, search warrants, etc.
2. Traffic stops including, but not limited to, traffic violations, stranded motorist assistance, and all crime interdiction stops.
3. Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording.
4. Code 3 responses.
5. Vehicle pursuits.
6. Prisoner transports.
7. Any other situation where audio and visual evidence would be of use.

(b) The body-worn camera system shall not be used to record non-business related activity.

(c) The body-worn camera system should not be activated in restrooms unless a specific business purpose requires its use.

(d) The body-worn camera system should not be activated at the Fremont Police facility without a specific business purpose.

(e) Personnel shall not activate the body-worn camera system device to record any personal conversation with or between other Department members or city employees.

(f) Personnel should not ordinarily activate the body-worn camera system when meeting with confidential informants.

(g) Sworn personnel are not required to obtain consent to record from a private person when:

Adoption Date: 2015/05/19

1. In a public place.
2. In a location where there is no reasonable expectation of privacy (e.g., inside a building or dwelling where personnel are lawfully present and engaged in the performance of official duties).

(h) Under sensitive circumstances, personnel should consider whether to advise private persons they are recording such as in a home, place of business, or during the rendering of medical care.

447.4.1 CESSATION OF RECORDING

(a) Once activated, the recording should continue until the officer reasonably believes the encounter has concluded, the situation has stabilized, or further recording would not be of evidentiary value. The officer may halt the recording in accordance with this policy, in between interviews, or when directed by a supervisor.

(b) Officers may cease recording when encountering or interviewing a victim who is in a vulnerable position or who asks not to be video-recorded.

(c) Officers may cease recording when interviewing a subject who does not want to be video-recorded and the officer feels obtaining the information or statement exceeds the importance of video evidence.

(d) In all cases above, the officer should verbally express the intent to stop recording prior to turning off the equipment, and should verbally express it has resumed if later reactivated. The officers should consider whether activating another type of recording device, such as audio recording would be appropriate for memorializing the interaction.

447.5 OPERATION

(a) Only trained personnel shall operate the body-worn camera system.

(b) Personnel shall not remove, dismantle or tamper with any hardware and/or software component or part of the body-worn camera system.

(c) Personnel shall position the camera on the front of their uniform to facilitate optimum recording field of view.

(d) The body-worn camera system must be manually activated.

(e) Personnel should dock their issued camera for automated upload of body-worn camera system data files daily at the end of their shift at the docking station to ensure storage capacity is not exceeded and/or to view uploaded audio/video.

447.6 REVIEW OF BODY-WORN CAMERA SYSTEM FILES

(a) Although the data captured by the body-worn camera system is not considered Criminal Offender Record Information (CORI), it shall be treated in the same manner as CORI data. All access to the system is logged and subject to audit at any time. Access to the data from the system is permitted on a right to know, need to know basis. Employees authorized under this policy may review video according to the provisions of this policy.

(b) Once uploaded to the server, personnel may view their own audio/video data at a department desktop computer and documenting the reason for access in the "NOTES" section prior to viewing any data. Access is automatically time/date stamped and records each access by name.

(c) An employee may review their own recorded body-worn camera system files under the following circumstances:

1. For the purpose of completing a criminal investigation and preparing official reports.
2. To prepare for courtroom testimony or courtroom presentation.
3. Following a critical incident: with supervisor approval, refer to Officer-Involved Shooting/Great Bodily Injury Incidents policy (310).
4. For potential training purposes.

(d) Supervisors may review all video files when there is a legitimate business purpose.

447.7 BODY-WORN CAMERA SYSTEM FILE REQUESTS

(a) Unauthorized use, duplication, and/or distribution of body-worn camera system files are prohibited. Personnel shall not make copies of any body-worn camera system file for their personal use and are prohibited from using a recording device such as a personal camera or any secondary video camera to record body-worn camera system files. All recorded media, images and audio are property of the Fremont Police Department and shall not be copied, released, or disseminated in any form or manner outside the parameters of this policy without the expressed written consent of the Chief of Police.

(b) Departmental requests, including requests from the District Attorney's Office or City Attorney's Office, shall be forwarded as a written request via e-mail, to the Property Unit, with sufficient information to locate the body-worn camera system file.

(c) Non-Department Requests

1. All other requests for a body-worn camera system file shall be accepted and processed in accordance with federal, state and local statutes and departmental policy (court cases, subpoenas, Release of Records and Information requests, etc.).
2. Media and/or Public Records Act requests shall be received and processed in accordance with federal, state, local laws and departmental policy.

3. When practical, personnel will be advised prior to any release of video under the CPRA (California Public Records Act) and the guidelines consistent with departmental policy.

(d) Request for Deletion of Accidental Recording

1. In the event of an accidental activation of the body-worn camera system, the recording employee may request that the body-worn camera system file be deleted by submitting an e-mail request with sufficient information to locate the body-worn camera system file to the Patrol Division Commander, who shall review the file, approve or deny the request, and forward to the System Administrator for action.

(e) Copying Procedures

1. A copy of the body-worn camera system file can be requested in accordance with the provisions of this policy.
2. Property Officers will be responsible for handling evidence requests for DVD copies and online sharing of files produced by the body-worn camera system system for court and other approved requests by the Chief of Police or his/her designee.
3. Property Officers will make a notation of the requestor and reason for each download, in the Evidence.com system.

(f) Investigators conducting criminal or internal investigations shall advise the System Administrator to restrict access/public disclosure of the body-worn camera system file in criminal or internal investigations, when necessary.

(g) A body-worn camera system file may be utilized as a training tool for individuals, specific units, and the department as a whole. A recommendation to utilize a body-worn camera system file for such purpose may come from any source as outlined below:

1. A person recommending utilization of a body-worn camera system file for training purposes shall submit the recommendation through the chain of command to the Patrol Division Commander or designee.
2. If an involved officer or employee objects to the showing of a recording, his/her objection will be submitted to staff to determine if the employee's objections outweigh the training value. The Patrol Division Commander or designee shall review the recommendation and determine how best to utilize the body-worn camera system file considering the identity of the person(s) involved, sensitivity of the incident, and the benefit of utilizing the file versus other means (e.g., department policy, Training Bulletin, Officer Safety Bulletin, briefing or other training).

PORTABLE VIDEO CAMERA POLICY

450.1 PURPOSE AND SCOPE

A. The purpose is to provide policy and procedures for the use of the Portable Video Recording System (PVRS), including both audio and video recording of field activity in the course of official police duties.
B. The use of the portable video recording system provides documentary evidence for criminal investigations, internal or administrative investigations, and civil litigation. Personnel shall utilize this device in accordance with the provisions in this policy to maximize the effectiveness of the audio/video documentation to achieve operational objectives and to ensure evidence integrity.

450.2 DEFINITIONS

A. PERSONNEL
Any uniformed (Class "B" and "C" which includes the bicycle uniform) personnel employed with the San Leandro Police Department.
B. ROUTINE
During the course of one's duties.
C. PVRS DEVICE
The Portable Video Recording System is an on-body video camera.

450.3 POLICY

A. Unauthorized use, duplication, and/or distribution of PVRS files are prohibited. Personnel shall not make copies of any PVRS files for their personal use and are prohibited from using a recording device such as a personal camera or any secondary video camera to record PVRS files. All recorded media, images and audio are property of the San Leandro Police Department and shall not be copied, released, or disseminated in any form or manner outside the parameters of this policy without the expressed written consent of the Chief of Police.
B. The PVRS shall not be used to record non-business related activity and shall not be activated in restrooms.
C. Only trained personnel shall operate PVRS equipment.
D. All personnel who are assigned a PVRS shall wear the device during any regular shift, any overtime shift and when the Chief of Police or their designee deem it appropriate to wear. Personnel will use only the PVRS issued and approved by the Department. The wearing of any other personal video recorder is not authorized.
E. Personnel shall not remove, dismantle or tamper with any hardware and/or software component or part of the PVRS.
F. There are many situations where the use of the PVRS is appropriate. This policy is not intended to describe every possible circumstance. Personnel may activate the system any time they feel its use would be appropriate and/or valuable to document an incident. Unless it is unsafe or impractical to do so, personnel should consider activating their PVRS cameras prior to making contact in any of the following incidents:

1. Enforcement encounters where there is a reasonable suspicion the person is involved in criminal activity. This includes, but is not limited to, dispatched calls as well as self-initiated activities.
2. Probation or parole search.
3. Service of search or arrest warrant.
4. Vehicle pursuits (as soon as practical).
5. K9 deployments, (e.g., cover officers, perimeter officers, etc.)
6. Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording.

G. Personnel may activate the PVRS before or during any other incident at their discretion.
H. During the activation, the recording should not be intentionally terminated until the conclusion of the encounter.
I. Personnel shall not activate the PVRS recording functions in any of the following incidents:

1. To record any personal conversation of/or between another department member and employee.
2. Personnel taking a report or conducting a preliminary investigation who reasonably believe no criteria for activation is present.
3. Personnel meeting with any Confidential Informants.

J. Sworn personnel are not required to obtain consent from a private person when:

1. In a public place.
2. In a location where there is no reasonable expectation of privacy (e.g., inside a building or dwelling where personnel are lawfully present and engaged in the performance of official duties).

K. Sworn personnel are encouraged to advise private persons they are recording if the advisement may gain compliance, assist in the investigation, and does not interfere with the investigation or officer safety.
L. SWAT personnel who are issued a PVRS and are engaged in an active SWAT entry, shall defer to the SWAT supervisor or incident commander for direction on the activation of the PVRS.
M. CID personnel who are issued a PVRS and who are preparing to engage in a probation, parole, arrest or search warrant entry shall wear the PSVRS on their outer vest carrier. They should also consider activating their PVRS cameras prior to making such entry and should continue recording until the situation becomes static. CID personnel should also consider using a PVRS when they deem it necessary during the course of any investigation.

450.4 RESPONSIBILITIES

A. The System Administrator is designated by the Chief of Police and has oversight responsibilities to include, but are not limited to, the following:

1. Operation and user administration of the system.
2. System evaluation
3. Training
4. Policy and procedure review and evaluation.
5. Coordination with IT regarding system related issues.
6. Ensure PVRS files of evidentiary value are secured and maintained for a minimum of one year. Ensure all other routine files (routine files are any files that are not assigned a report number) are secured and maintained for 90 days.
7. Ensure PVRS files are reviewed and released in accordance with federal, state and local statutes and the City of San Leandro/San Leandro Police Department retention policy.

B. Supervisory

1. Supervisors will ensure personnel utilize the PVRS according to policy guidelines.
2. Managers may conduct periodic audits of recordings to ensure adherence to policy, assess performance and for training purposes. Audit will be fair and impartial.
3. Officers will have the ability to audit any of their videos at their discretion. Officers may contact the System Administrator if they feel videos were viewed against policy.
4. The POA President or his/her designee may review the audit log with reasonable notice through the Office of the Chief of Police to ensure the audits are conducted fairly. At no time will the audit log be duplicated or distributed.

C. Personnel utilizing the PVRS are responsible for the following:

1. Ensuring the battery is fully charged and operating properly.
2. Immediately report unresolved equipment malfunctions/problems to their supervisor.
3. Documenting the use of the PVRS on one of the following:
   - In the police report/CAD entry.
   - As a notation on a citation.
   - On a field contact card.
4. Once video is captured, officers should identify the PVRS files:
   - When assigned, noting the San Leandro Police Department case number in the Case ID Field.
   - Entering a title. The title should include sufficient information to identify the file, such as crime code, suspect name, location, event, etc.
   - Selecting the appropriate category(s).
   - The information may be entered via hand held device, Mobile, or SLPD computer workstation before the end of the shift.

450.5 OPERATION

Any time that an officer records any portion of a contact which the officer reasonably believes constitutes evidence in a criminal case; the officer shall record the related case number and book the recording media into evidence or download the file in accordance with current procedure for storing digital files.

A. The officer shall further note in any related report that the recording has been placed into evidence.
B. Recording media placed into evidence shall be retained through the final disposition of the related criminal case.

450.5.1 NON-CRIMINAL MATTER

Any time that an officer reasonably believes that a recorded contact may be of benefit in a non-criminal matter (e.g., a hostile contact), the officer may book the recording media into safekeeping or download the file in accordance with the current procedure for storing digital files.

A. Under such circumstances, the officer shall notify a supervisor of the existence of the recording as soon as practical. Recording media which has been placed into safekeeping shall be retained for a period of not less than 180 days or until the related matter has been closed (e.g., internal investigation, civil litigation).

   Once any recording medium has been filed, the officer shall place it into safekeeping or download the file in accordance with current procedure for storing digital files where it shall be retained for a period of no less than 180 days unless utilized in a specific case.

450.6 REVIEW OF RECORDED MEDIA FILES

A. Although the data captured by the PVRS is not considered Criminal Offender Record Information (CORI), it shall be treated in the same manner as CORI data. All access to the system is logged and subject to audit at any time. Access to the data from the system is permitted on a right to know, need to know basis. Employees authorized under this policy may review video according to the provisions of this policy.
B. Once uploaded to the server, personnel may view their own audio/video data at a department desktop computer and documenting the reason for access in the “Notes” section prior to viewing any data. Access is automatically time/date stamped and records each access by name.
C. An employee may review PVRS files as it relates to their involvement in:

   1. An incident for the purpose of completing a criminal investigation and preparing official reports.
   2. Prior to courtroom testimony or for courtroom presentation.

3. In the event of a critical incident:

    - All PVRS recordings shall be uploaded to the server as soon as practical.

    - During this critical incident, the initial interview of an involved officer should occur before the officer has reviewed any audio/video recordings of the incident. An involved officer will have the opportunity to review recordings after the initial statement has been taken. Should the Investigators decide not to allow the officer(s) to view the recordings prior to the initial interview; the involved officer(s) attorney(s) may have the opportunity to review the recordings prior to the initial interview. Investigators should be mindful that audio/video recordings have limitations and may depict events differently than the events recalled by an involved officer. If the Investigator shows any audio/video recordings to an involved officer after the initial interview, the Investigator has the discretion to admonish an involved officer about the limitations of audio/video recordings.

    The following is an example of an appropriate admonishment in a case involving video evidence:

    > "In this case, there is video evidence that you will have an opportunity to view after you have given your initial statement. Video evidence has limitations and may depict the event 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. 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 initial statement explains your state of mind at the time of the incident".
    >
    > Investigators may ask an involved officer to view the incident scene during a "walk through." The Investigator will determine the timing of the "walk through", however, it should not occur prior to the initial statement of an involved officer. Only one involved officer at a time will be permitted to do a "walk through" of the scene.

4. For potential training purposes.
5. Personnel may view all video that they appear in, either visually or audibly. Additionally, personnel may view other personnel's video, when they were not seen or heard in the video if they have a similar perspective or were in close proximity of any functioning PVRS's.

D. Personnel with investigatory responsibilities may review PVRS files under the provisions of this policy for the purpose of conducting official departmental business.

450.7 PVRS FILE REQUESTS

A. Departmental requests to include requests from the District Attorney's Office or City Attorney's Office, shall forward a written request via e-mail with sufficient information to locate the PVRS file to the system administrator.

B. Non-Department requests:

1. All other requests for a PVRS file shall be accepted and processed in accordance with federal, state and local statutes and departmental policy (court cases, subpoena's, public records act, etc.) as set forth in Lexipol Policy #810 (Release of Records and Information).
2. Media inquiries and/or requests shall be received and processed in accordance with Lexipol General Operations #346 (News Media Relations).
3. When practical, personnel will be advised, prior to any release, of video under the CPRA (California Public Records Act) and the guidelines consistent with Lexipol Policy #810.

C. Request for Deletion of Accidental Recording
In the event of an accidental activation of the PVRS, the recording employee may request that the PVRS file be deleted by submitting an e-mail request with sufficient information to locate the PVRS file to the Operations Division Captain or designee who shall review the file, approve or deny the request, and forward the request to the Professional Standards Unit for action.

Copying Procedures require a PVRS file be requested in accordance with the provisions of the order by submitting a written request to the System Administrator including the reason for the request.

Investigators conducting criminal or internal investigations shall advise the System Administrator to restrict access/public disclosure of the PVRS file in criminal or internal investigations, when necessary.

D. A PVRS file may be utilized as a training tool for individuals, specific units, and the department as a whole. A recommendation to utilize a PVRS file for such purpose may come from any source as outlined below:

1. A person recommending utilization of a PVRS file for training purposes shall submit the recommendation through the chain of command to the Operations Captain or designee.
2. If an involved officer or employee objects to the showing of a recording, his/her objection will be submitted to staff to determine if the employee's objections outweigh the training value.
3. The Operations Captain or designee shall review the recommendation and determine how best to utilize the PVRS file considering the identity of the person(s) involved, sensitivity of the incident, and the benefit of utilizing the file versus other means (e.g., General Order, Training Bulletin, Officer Safety Bulletin, briefing or other training).

450.8 REPAIR PROCEDURE

A. Personnel should immediately report any problems with the PVRS to their immediate supervisor.
B. Upon notification, the supervisor shall contact the System Administrator or designee stating the problem or malfunction.