Testimony of Vincent Talucci
Executive Director/Chief Executive Officer
International Association of Chiefs of Police

Before the Task Force on 21st Century Policing
Listening Session: Technology
January 31, 2015

Commissioner Ramsey, Professor Robinson, Director Davis and members of the Task Force on 21st Century Policing, thank you for inviting me to testify today. My name is Vincent Talucci and I am the Executive Director at the International Association of Chiefs of Police (IACP).

The IACP is the world's largest association of law enforcement executives, with more than 22,000 members in 98 different countries. For over 120 years, the IACP has been launching internationally acclaimed programs, speaking out on behalf of law enforcement, conducting ground-breaking research, and providing exemplary programs and services to the law enforcement profession across the globe. One of the services we provide is developing and refining model policies for law enforcement on complicated issues like the use of technology.

The IACP released a model policy on body worn cameras in April of 2014 and published a technology policy framework that addresses a broad spectrum of emerging technologies and privacy and civil liberties concerns. Both of these documents incorporate the research findings, the input of leading subject experts, and the professional judgment of advisors who have combined this information with their extensive practical field and management experience.

There is no question that new and emerging technologies, like body worn cameras, play an increasingly 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. In a time when law enforcement agencies are typically operating with a reduced force and agencies are asking their officers to respond to an ever expanding variety of calls for service, the use of technology has become essential.

Given calls for greater transparency and increasing scrutiny of law enforcement operations and performance, particularly in light of recent events, agencies need to implement technology that supports and enhances transparency in police-community interactions in order to promote public confidence and aid in a meaningful dialogue between law enforcement and the community.

Today I am focusing primarily on the use of cameras—and specifically body-worn cameras—because that has become the principal technology people are turning to in documenting police community-relations. I would like to emphasize that this certainly does not fully encompass the breadth of technology that can assist agencies, but evidence suggests that when body-worn cameras are implemented thoughtfully and with proper planning and management, that it holds significant promise in influencing behavior, providing transparency and accountability, and documenting critical interactions between police and citizens.

Video recorders and digital cameras have been useful tools in the law enforcement profession for some years. The concept of recording police-citizen encounters for law enforcement use first developed with the implementation of in-car cameras. Continual advances in technology has enabled industry to engineer smaller, lighter, more powerful, and more mobile digital camera equipment and enhanced the development of the body-worn cameras (BWC).

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, objective account of what was said and done during an incident. The utilization of BWC video and audio recordings at trial can provide the court with the document of the actual statements and behavior of officers, suspects, and others that might not otherwise be admissible in court based upon hearsay rules, 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 jurisdictions an additional means of defending themselves in civil litigation. Video evidence 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. An officer utilizing a BWC, however, 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. In one study, a Police Department found that in cases where video evidence was available, the officer was exonerated 93% of the time; in 5% of the cases the complaint was sustained. In addition, the same study showed that in a large number of instances, the citizen decided against filing a complaint once he or she was notified that there was a video recording of the incident.

To be fair, BWCs can also provide needed evidence of wrongdoing or inappropriate behavior on the part of an officer, in those rare cases where a complaint is sustained. Moreover, the video, whether taken from the in-car camera or the BWC, can also document behaviors and practices that need to be addressed in training. There have also been far too many instances in which in-car and body-worn cameras have captured the tragic death or serious injury of an officer, and the video images captured are the conclusive evidence of these desperate acts.

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 that when they inform the subject that they are being recorded by video and/or audio means, the fact 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. In a one-year study conducted by the Rialto Police Department (CA), citizen complaints of officer misconduct fell by 87.5 percent for officers using BWCs, and the number of use of force incidents decreased by 60% department-wide during the year in which they piloted body worn cameras. The Mesa Police Department (AZ) had similar outcomes as they evaluated their body-worn camera program, with 40% fewer complaints against officers assigned to wear body cameras and 75% fewer complaints against these officers regarding their use of force.

Although I have just outlined several benefits to the use of video recording devices, they are not the sole solution. For instance, civilians may see the videos differently than a police officer experiences the situation in real life. Police are watching for certain behaviors from suspects that a civilian may not be aware of and no video can truly capture the feeling of when an officer is put in a situation where he or she fears for their life. In addition, other factors that may not be caught on video might not paint the whole picture of the incident under review or in question.

In addition other factors play into account that the video may not capture, sun glare, action going on out of the videos range of view, etc.

I would also like to note that video recording devices and all other technologies are useless and perhaps even harmful unless they are properly deployed and implemented. Just because a technology *can* be implemented, doesn't mean that it *should* be implemented. Law enforcement agencies must create and enforce comprehensive agency policies governing the deployment and use of these technologies, and the data they provide, if they are going to be successful.

Prior to the use of any technology, like BWC's, dash-cams, automatic license plate readers, etc., agencies need to have policies in place that govern the deployment and use of the technology. Moreover, the policies must address how the agency will protect the civil rights and civil liberties of individuals, as well as recognize and respect the privacy protections regarding the data collected, stored, and used. Development and enforcement of these policies is essential to effective and sustainable implementation, and to maintaining community trust.

That is why the IACP took the lead in developing a technology policy framework to identify universal principals that can be used as a guide to all law enforcement agencies as they develop effective policies for the use of technologies. Those principles include:

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.

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.

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.

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.

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.

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.

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), 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.

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.

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.

I have already mentioned both the Mesa (AZ) and Rialto (CA) police departments that have implemented body-worn camera technology and have experienced positive results. Other

agencies like the Los Angeles (CA) Police Department, Seattle (WA) Police Department, and Chicago (IL) Police Department are either in the process of conducting pilot programs are going to be partaking in pilot programs for body-worn cameras. These agencies are going about this process in a well-calculated and thoughtful way. It is imperative that any agency that plans to roll out this technology do so by testing it out first and thinking about important elements like privacy, when officers are required to turn on their cameras, what the protocol will be for interviewing victims, providing officers with training, etc.

Another good example of an agency that has used non-lethal technology to enhance officer safety and safeguard the public is the Philadelphia (PA) Police Department and its use of electronic control weapons. The Philadelphia Police Department successfully blended both policy and technology, through the by the completion of Crisis Intervention Training (CIT) with issuance of electronic control weapons. This ensures that all officers authorized to deploy electronic control weapons have had training in the intricacies of crisis intervention and are educated in protocols of responding to situations involving individuals with mental illness.

While technology has proven to be a useful tool for law enforcement, we must remember, that technology can both facilitate and inhibit building community bonds. The benefits that technology can bring to law enforcement and their relations ship with the community 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.

We must also be mindful, that although the economy has substantially recovered, a lot of that recovery has not trickled down to local governments and law enforcement agencies. If the members of the Task Force decide that it is necessary for all agencies to acquire certain technologies, there needs to be resource assistance to do so.

Again, thank you for convening this listening session and for the opportunity for the International Association of Chiefs of Police to express its views on the use of technology to aid in the strengthening of community-police relations in the United States. I do hope that you will get a chance to read our technology policy framework and our model policy on the use of BWCs. I welcome any questions from Task Force members.

Appendix

Model Policy

Effective Date	*Number*
April 2014	

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.

[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. 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 data (images, sounds, and metadata) 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.

[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 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 a grant 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 was designed to accompany the *Model Policy on Body-Worn Cameras* established by the IACP National Law Enforcement Policy Center. This paper provides essential background material and supporting documentation to provide 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 community and their law enforcement agency.

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

[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.

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

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 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.

[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.

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.

---

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

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.

---

[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.*

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.

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 a grant 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 *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*

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.

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.