A Snapshot of the IG Implications for

BODY-WORN CAMERAS

Police officers' video recordings of activities and people in public spaces via their body-worn cameras (BWC) have been at the center of many recent controversies – becoming one of the most vehemently debated uses of information technologies ever. This article focuses on the information governance implications of BWC.

John T. Phillips, CRM, CDIA, FAI

Though accurately captured and properly managed digital video recordings of law enforcement-public interactions via body-worn cameras (BWCs) have great potential for creating objective data useful for legal system evidence, dispute resolution, historical documentation, and regulatory records management, they also pose some of the most complex social and technical issues of any modern recordkeeping technologies.

BWC's Social Issues

BWC systems were intended as a tool to assist police investigations and provide records regarding officers' actions and interactions while conducting patrols. Implementing them for that purpose provided the usual lessons learned from any IT systems implementation, including needed functionality for officers, comprehensiveness of data gathered, length of time needed for data storage, and the utility of the evidence gathered.

While BWC technology is of great use to police officers and their supervisors for management purposes, the existence of BWC-gathered electronic data also sparks an interest on the part of the public, legal system professionals, and government oversight agencies.

Effect on Public/Police Trust

BWC videos can impact the outcomes of police/public interactions with consequences for both groups, potentially putting the safety and security of both at risk if the videos are misused or released inappropriately.
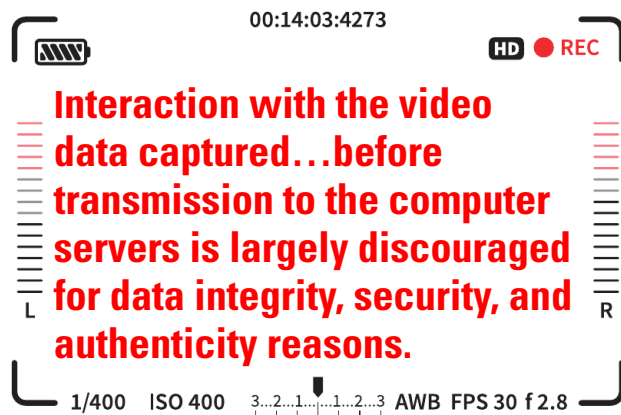
As a result of national news media coverage of U.S. police/public interactions that feature BWC video, as well as citizens' video recordings, public trust in law enforcement has sometimes been broken with devastating consequences for communities. Several incidents, such as the violence that arose after a 2014 police shooting in Ferguson, Missouri, have sparked a national debate about the use of BWC by police departments and the video records created.

Believing that had BWC-video been in use by the Ferguson Police Department, the unrest that occurred might have been mitigated, many police departments rushed to equip themselves with this technology. Securing the technology, though, is just the first step for law enforcement. It is imperative for agencies to address these questions about BWC records creation, collection, and management that have arisen from these debates, including:

1. Can an officer control (turn on/off) the camera?
2. When does a camera begin gathering data?
3. Can an officer direct the focal view of the camera?
4. What happens to the video stream captured during an officer's shift?
5. Is the captured video stored locally or in the cloud?
6. How soon is the data available for requests from outside the police department?
7. Must the video data be subjected to review internally before release?
8. Is redaction of identities performed before release to ensure compliance with privacy laws?
9. Is use of a BWC by officers optional?
10. Is there a publicly supported policy in place regarding the use of BWCs?

Police departments that implement BWCs must develop a policy that supports the operational needs of those charged with using them while remaining accountable to the demands from the public, the media, and attorneys.

If departments fail to create records management policies regarding BWC-captured digital files, another unanticipated outcome can be inconsistent responses to records requests, which can create a trust failure with the public – the opposite of the departments' intention to improve that trust through their procurement of a BWC system.

00:14:03:4273

▓▓▓▓   **HD ● REC**

Interaction with the video data captured…before transmission to the computer servers is largely discouraged for data integrity, security, and authenticity reasons.

L   R

1/400   ISO 400   3…2…1…│…1…2…3   AWB FPS 30 f 2.8

BWC's Technical Issues

Because BWC-captured video has the potential for portraying police and public actions positively or negatively, BWC systems must be effectively designed and rigorously implemented in accordance with police department recordkeeping practices and public expectations to be effective, economically viable, and perceived as non-partisan.

Any agency intending to use BWC technology should plan to address early in system design, selection, and implementation the social impact on communities, adherence to open records laws, privacy regulations compliance, and data retention issues.

System design issues must include planning for the impact of public records laws, demands from attorneys and courts, police department staffing and budgets, and long-term data management and storage.

Operational System Design

BWC systems are intended to record actions occurring in front of police officers while they conduct their daily business. This requires BWCs to be focused on the landscape in front of an officer and to record at a sufficient rate and video resolution to create good records.

Data can be recorded locally on each camera or can be directly transmitted to remote computer servers that store the data. Microphones must be operational and able to record audio occurring near or in front of the officers.

Many functional and system design technical issues can affect the utility of BWCs and the success with which they can meet operational requirements. Typical functional requirements that could affect records creation and preservation are identified by the U.S. Department of Homeland Security System Assessment and Validation for Emergency Responders (SAVER) program "Body-Worn Cameras for Law Enforcement Assessment Report" (*https://www.dhs.gov/sites/default/files/publications/Body-Worn-Cams-AR_0415-508.pdf*). They include:

1. Head vs. body mounting vs. field of view when an officer is standing sideways
2. Recording duration in hours and minutes per battery charge
3. On-board data storage capacity in gigabytes based on capture resolution
4. Proprietary software use and video data formats
5. Data security, audit trail, and activity logs

Operational Use Recommendations

Of particular importance to the use of BWCs is the management of the data once it is captured on an operating camera.

Officer Review of Video

Interaction with the video data captured by an officer before transmission to the computer servers is largely discouraged for data integrity, security, and authenticity reasons. Though there may be some instances requiring immediate review of video, interaction with the data being captured can raise evidentiary and chain of custody issues. For this reason, there are benefits to having officers not involved in immediate review and management of the data captured.

In contrast, officer participation in subsequent review

of captured video is often critical to providing general understanding of content, video metadata regarding context, GPS/location information, and specific identification of individuals.

Privacy Review of Video, Redaction

Video captured in public settings also must be appropriately reviewed before its release to the public to ensure data privacy and personal security issues are considered. For example, release of personally identifiable information regarding minors, including their facial appearances, is typically unlawful. In addition, the identification of suspects or victims of crimes can place those individuals, as well as police officers with BWCs, at risk. For this reason, video redaction software and strict video review policies must be in place and rigorously practiced.

Dedicated Resources Needed

The costs for capturing and initially recording BWC records can be high due to the need to fund well-planned systems design, initial camera acquisition, and any general IT infrastructure improvements. These are largely one-time, up-front costs to begin operations, but they could continue for a few years.

Capturing BWC data also can place a large operational burden on police departments if there are not enough staff and resources to properly manage this influx of electronic records. Many records created during "the normal course" of police business are subject to U.S. federal and state open records laws, creating public expectations, legal system demands, and astronomical costs that police departments may not have anticipated when planning their BWC system.

As often occurs when there is public or news media demand for information considered to be a public record, there must be sufficient departmental and IT systems staffing set aside for sudden workload increases. Often rivaling the volume of requests for captured e-mail and social media records, requests for BWC-created records can make implementing BWC systems cost prohibitive.
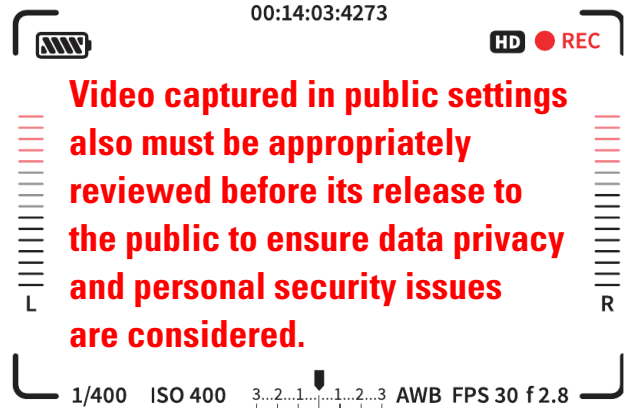
Thus, in addition to the hardware, software, and other technology infrastructure costs associated with implementing BWCs, there must be additional departmental resources allocated to ensure overall recordkeeping goals are met. These issues alone have discouraged many urban police and county sheriff's departments from deploying BWC technologies.

Retention and Storage Issues

Post-implementation, major concerns are the longer-term IT infrastructure and funding issues related to electronic records retention and data storage capacity. A September 11, 2016, Associated Press (AP) article by Rick Callahan cited the cost of state-mandated video retention requirements as the reason police departments in Indiana and Connecticut shelved their BWC programs.

For example, in Clarksville, Indiana, Police Chief Mark Palmer said a state law that took effect on July 1 last year raised the minimum retention of BWC video

00:14:03:4273

Video captured in public settings also must be appropriately reviewed before its release to the public to ensure data privacy and personal security issues are considered.

from 30 days to 190 days and would have skyrocketed the video storage and camera maintenance cost for his department's four-year-old program – from $5,000-$10,000 a year to $50,000 - $100,000. Additional servers, cameras, software, and training to implement the change would have added significant additional costs for the town of 20,000 residents, Palmer was quoted as saying in the AP article.

Data storage costs can be estimated by recognizing the digital file sizes being created (and disk space consumed) based on a camera's video capture resolution, multiplied by the average number of video files created per hour on a typical officer's work shift, multiplied by the number of officer hours being logged per week or month.

The internal IT costs to support this level of data storage can be estimated from a request for proposals for outsourced data storage services. The potential to reduce storage costs by altering systems with respect to data capture or number of hours of video recorded can be counterproductive, as this also can lower system usefulness and performance levels. The most direct way to reduce video records storage costs is to reduce the volume of records stored by reducing the length of time for which records are retained.

Records retention policy, especially with respect to the duration of records retention, can be influenced by many factors, including regulatory and legal mandates like the one mentioned above in Kentucky. Several states have set mandatory retention periods for BWC video; the National Conference of State Legislatures maintains a BWC laws database that reveals which states, along with many other regulatory and legal requirements, at *www.ncsl.org/ research/civil-and-criminal-justice/body-worn-cameras-interactive-graphic.aspx.*

The requirements to ensure appropriate privacy protection are addressed before releasing video, such as masking the identities of juveniles and potential witness-

es as mentioned above, can result in creating and maintaining additional copies of a video – the original video record and any copies created for release to the public or for use in legal settings. Thus, data storage for video files can quickly double based on the need for multiple copies.

These types of decisions should be made with input from qualified professionals, including legal counsel and records management staff. Unfortunately, it is common for police departments to run out of initially planned data storage within a few months of system initiation, resulting in the use of flexible cloud-based data storage to continue operations.

In fact, Taser international, a cloud-based BWC system vendor, recently stated that it derives gross profit margins on hardware (cameras) of 15.6% while gross profit margins on video storage are about 51%. As an example, the Birmingham, Alabama, Police Department said in a September 2015 *Computerworld* article that the five-year contract for camera cost was estimated to be $180,000, while the overall cost – including data storage – would be $889,000. For this reason, planning records retention policy and data storage capacity are critical to the long-term viability of BWC systems.

Information Governance Issues

When organizations implement IT systems, they must incorporate plans to manage the information for later retrieval, considering both immediate and long-term information governance (IG) issues. BWC systems are frequently implemented in reaction to media-publicized events in the hope of better documenting police interactions with the public and public actions during community events. The video and audio information created must be produced responsibly and managed well to ensure its proper retention and preservation. Retention rules, data management policies, and chain of custody expectations must be designed into the operational requirements for a BWC system to ensure that it meets overall expectations.

To ensure the ability to respond to public records requests or subpoenas effectively, police departments must get input into the BWC system design from public records advocates, attorneys, archivists, and police department records managers. Factor this input into system design to ensure proper IG, and show these criteria during budget planning efforts to ensure that adequate resources and personnel are available to meet expectations. Identify the costs for long-term storage of these records and the resources needed to provide public access, and get funding early to avoid budgetary and resources challenges after the system is operational.

Police officers on patrol are often seen as the "end user" who should determine whether a BWC system is "user friendly." Tremendous consideration should be given to the impact of adding a technical responsibility to their already-demanding roles in public safety and security. But, remember that there will eventually be another set of "end users" for the video data: public information seekers, news media, and courts.

Considering in advance of system implementation the long-range considerations for governing this new treasure trove of information will greatly enhance the utility and viability of this body of electronic records. **E**

About the Author: John T. Phillips, CRM, CDIA, FAI, has made a major difference in the ability of individuals to remain knowledgeable about changing information management methodologies and technologies for many years. He is a consultant with Information Technology Decisions, author, and educator, and his work illustrates how information management professionals can grow as their professional activities increasingly include electronic records. A Certified Records Manager, Certified Document Imaging Architect, and Fellow of ARMA International, Phillips can be contacted at *john@infotech decisions.com*.