Redbooks
ibm.com/redbooks

Improving Police "Body Cam" Programs with an End-to-End Solution

Richard Budel
Peter Coldicott
Steve Correl
Don Dejewski
Mark Dixon
Peter Williams

In partnership with
IBM **Academy of Technology**

IBM

Redpaper

Introduction

Policing in the 21st Century saw major advances in technology and operational efficiency and an increased focus on accountability. Citizens play a huge role in the equation as critical first communicators at crime and accident scenes. The perspective of the law enforcement officer (LEO) is equally vital. And today, that perspective is frequently, and increasingly, captured by using body-worn cameras (BWCs).

Yet, police BWC programs involve much more than just wearing cameras and recording video. Important additional concerns exist, too:

- The sheer volume of BWC video and the costs to store and manage it
- Camera streams that might consume limited communications bandwidth in emergencies
- The protection and preservation of BWC video for investigations and judicial proceedings
- The development and administration of complex BWC-related policies and procedures
- The ability to make BWC video accessible, securely, to appropriate internal and external viewers

It's evident, then, that an effective BWC program requires a well-managed, flexible, and policy-driven approach. It also requires a robust hardware and software infrastructure both to support the physical aspects of the program and help guide and enforce the all-important administrative policies.

This IBM® Redpaper™ publication aims to identify the key technical areas to address when a police agency deploys BWCs. However, rather than focus on the camera itself, we describe a powerful IBM platform that provides an end-to-end solution to help police agencies manage their BWC programs, save money, and adhere to the growing list of rules that govern the use of BWCs.

The end-to-end IBM solution includes these critical functions:

- A single content management/video repository that supports digital evidence from multiple video sources and BWC technologies (IBM FileNet Content Manager with a video library tool)
- Records management software to apply rules for handling and retaining video (IBM Enterprise Records)
- Video analytics and redaction capabilities (IBM Intelligent Video Analytics)
- Storage options for the captured video, possibly including on-premises storage (IBM Elastic Storage™ Server and optionally, the IBM Linear Tape File System™ for direct access or archiving)

The paper focuses on BWCs that are used by law enforcement agencies. Yet, the discussion is also applicable to BWCs that are worn by first responders, the military, corporate security personnel, and others. We use BWC video and audio as the focal points. However, the topics that are addressed are equally relevant for other forms of mobile and field-based video/audio capture (such as dashboard cameras (dashcams) and smartphones) in locations, such as schools, correctional facilities, and elsewhere.

We start with a look at the current landscape for body-worn cameras to assess the major cost drivers and the current technologies that are provided by vendors of cameras and related digital asset management tools. We then describe a typical BWC lifecycle, which includes the following components:

- Video capture
- Video ingestion
- Searching
- Tagging
- Video analytics
- Storage
- Retention
- Archiving
- Playback

We outline how the components of the end-to-end IBM platform can address each phase. We conclude with a description of possible future scenarios for BWCs and explain how IBM can help achieve these goals.

Background and current landscape

Law enforcement officials were interested in BWC-captured video for many years, with the first BWC deployments in 2006.[1] More recently, following a number of high profile events in the United States and Europe where police conduct was called into question (primarily use-of-force (UoF) incidents and officer-involved-shootings (OIS)), the value of using video records of police activity is a hot topic.

Whether it is termed “seeing a situation as the police officer was seeing it” or “capturing the truth” about each encounter, a growing expectation exists that BWC video will be available. BWCs are becoming an increasingly common accessory (and in certain cities, a mandatory accessory) on the LEO’s tool belt.

Many BWC vendors exist. Among them, commonality emerged in terms of how the video is captured, but differences remain in both capabilities and approach. The cameras themselves can differ. They can be high definition or standard definition. They can be worn as clip-ons (typically mounted chest high), in eyeglass form, or as part of a headset. They might turn on automatically or need to be activated manually. The list goes on.

[1] Michael D. White, Ph.D, *Police Officer Body-Worn Cameras: Assessing the Evidence*, 2014, Office of Justice Programs Diagnostic Center, which is available at this website: http://bit.ly/1p5exDw

BWCs today

BWCs overwhelmingly ranked first among the technology priorities that face today's LEOs, according to a recent national survey that was conducted by the Public Technology Institute (PTI).[2] More than 62% of respondents stated that BWCs will be their highest technological priority over the next five years. The same study indicated that more than 34% of the responding agencies are considering deploying BWCs.

In terms of law enforcement activities, results vary. An initial report, which was based on 2012 data from the Rialto, California, police department, demonstrated immensely positive return on investment (ROI) from deploying BWCs. Rialto police saw a decrease of 60% in UoF incidents and a 90% reduction in complaints about police conduct.[3] However, several recent experiences show that the technology is not without challenges. A proof-of-concept project in Denver, Colorado, for example, showed an increase in both UoF incidents and the number of complaints against the police, with less than one third of the incidents captured on video.[4] In San Diego, California, an initial decrease in UoF incidents occurred in the first six months of BWC deployment, after which such incidents increased over the next six months, with an additional 36% rise in assaults against officers.[5] Although several problems in the Denver example were attributed to policy and cultural issues, these numbers serve as a reminder that BWC technology is still rapidly evolving. It is important to address the cultural and policy aspects, as well as technological aspects.

Many questions are still unanswered that will affect both the cost of BWC projects and their ROI. For example, debates are ongoing over the issue of video capture. When does the camera turn on and when does it begin recording? Who can turn off the camera, and under what circumstances? When and how is video shared with the public, and how much of it needs to be redacted?

Also, the human element must be considered, and the fundamental shift that BWCs impose on LEOs must be evaluated. BWCs can capture what the officer cannot. The field of view for these cameras ranges from 90 - 170 degrees in which everything can be captured at high definition (HD)-level quality. The human eye has a field of view of just 55 - 60 degrees, and it can narrow to 2 degrees in times of stress. Is it fair to use the 20/20 hindsight that is afforded by the unblinking camera to judge the actions of an LEO? Furthermore, a camera provides only a one-dimensional recording of a multi-dimensional situation. A universal set of standards is not available by which to judge the human perspective against the perspective of the camera. Likewise, the idea of blindly trusting the video as the authoritative source is attractive, but flawed.

---

[2] *2015 Local Government Law Enforcement Technologies: National Survey Results*, July 2015, Public Technology Institute (PTI), http://www.pti.org/civicax/inc/blobfetch.aspx?BlobID=22726

[3] Tod Newcombe, *For the Record: Understanding the Technology Behind Body Worn Cameras*, Sept. 8, 2015, GovTech.com (division of e.Republic, Inc.®), https://ibm.biz/BdHguL

[4] Sadie Gurman, *Denver body cams didn't record most use of force cases*, March 11, 2015, Associated Press, https://ibm.biz/BdHguC

[5] Tad Vezner, *Police body cameras making a difference? Still unclear*, Sept. 23, 2015, Pioneer Press (St. Paul, MN), http://www.twincities.com/localnews/ci_28865363/police-body-cameras-making-difference-still-unclear

Cost concerns

Putting technical and policy issues aside, the greatest consideration for law enforcement officials is typically the cost of a BWC deployment in terms of people, information technology, and so on.

Industry benchmarks place the ratio of administrative costs when compared to acquisition costs at between 8:1 and 10:1. Human tasks that might be underestimated include reviewing video, redacting parts that cannot be released, and managing public distribution of the video (such as is received in the United States through Freedom of Information Act (FOIA) requests). In Duluth, Minnesota, the initial acquisition cost of $5,000 for cameras was dwarfed by the estimated video storage cost of $78,000 yearly.[6] The mayor of Baltimore, Maryland, placed a hold on BWC deployment in early 2015 after the city estimated that the maintenance costs of BWC video might exceed $2.5 million yearly.[7] And in one seemingly extreme example, police in Wichita, Kansas, sold a helicopter to raise funds to sustain their BWC implementation.[8]

The following primary cost drivers of BWC programs also turn out to be the primary factors in making decisions about these programs:

- Acquisition, equipment, and maintenance
- Video storage and retention
- Video management, redaction, and retrieval
- Video analytics

Acquisition, equipment, and maintenance

With interest in the technology growing rapidly, the BWC market grows dramatically. BWC manufacturers are in a virtual arms race, offering more mobile models that can be positioned in various areas of the body and various new camera types (one-piece and two-piece systems, for example). In the same way that the mobile phone market progressed rapidly due to competition, BWC vendors are trying to leapfrog each other with features, such as longer battery life, enhanced resolution, lighter weight, improved low-light performance, and increased field of view. With prices for BWCs that range from $100 to $2,500, the adage that *you get what you pay for* holds true, and police forces face a difficult task to prioritize the features that are most important and cost-effective for them. Underlying it all is a fear that favoring any single camera, or vendor, today can result in technological obsolescence tomorrow.

Another challenge in this evolving market is the definition of an *end-to-end* solution. BWC vendors usually offer solid hardware solutions for the camera components, and they are now starting to provide solutions that are more comprehensive. Yet, questions still loom. What is included in the solution? Does it integrate with existing systems and technology (or other BWC solutions)? As more BWC manufacturers focus on protecting sensitive video with encryption and proprietary formats, what happens if an agency wants to integrate its video with other systems, such as video analytics, or if it wants to move to a new platform in three years? Is the data portable? Do they lose all of the metadata and analytics?

[6] Brian Bakst and Ryan J. Foley, *For police body cameras, big costs loom in storage*, Feb. 6, 2015, Associated Press, https://ibm.biz/BdHguQ
[7] Ibid.
[8] Ibid.

Video storage and retention

How to manage the flood of BWC data is the number one concern for agencies that seek to deploy BWCs. Many agencies struggled to effectively manage the video that came from in-car cameras (such as cameras that are mounted on dashboards), but discovered low-cost methods to offload the data onto DVDs or portable hard disk drives.

In contrast, BWC footage presents two problems. First, the volume of data that is captured is greater than the volume of data from in-car video. If a single BWC device records at 720p for most of an LEO's 12-hour shift, a single BWC device can create 300 GB or more of video data each month. Second, because BWCs are mobile and they can be used inside a home or during an interview of potential victims, the privacy requirements that relate to BWC video dictate much higher levels of care and maintenance[9], both of which increase costs. As police agencies, such as San Diego's police agency, struggle to raise funds for their estimated $3.5 million in storage costs[10], and Oakland police try to manage the 7 TB of data that is created each month from their 600 cameras[11], cloud-based hosting with its easy rollout and funding model (*operational* expenditures (op-ex) versus *capital* expenditures (cap-ex)) gains increasing attention.

Agencies also need to establish review and retention policies for video that is collected by BWCs. Video of even a simple traffic stop might need to be retained for months while the case moves through the judicial system. Video from an actual traffic accident or a driving while intoxicated (DWI) arrest, if it involves felony arrest or detailed investigation, might need to be retained for years, or sometimes *forever* (at least for the life of the suspect or until all appeals are exhausted). And what about video that is captured but is not related to any active or current case? How long do you need to retain this type of video? Does it possess ongoing value? Or is it a risk to the agency or municipality if it is retained and later becomes the subject of litigation?

Video management, redaction, and retrieval

The nature of BWC video is often intimate and personal, which makes it different from dashcam video or closed-circuit TV footage. Agencies are currently wrestling with this issue and trying to balance the right of free public access (because the video is captured in public by using publicly owned devices that are funded by public tax monies) with the right to privacy that individuals presumably can expect in their interactions with law enforcement.

The outcomes of these policy discussions have major cost implications: How long must video be retained (particularly because the more video that is retained, the higher the cost of the storage)? How much time and money must be spent redacting (blurring or removing) portions of BWC video to protect someone's privacy? How much time will be consumed responding to Freedom of Information Act (FOIA) requests? The Seattle (Washington) Police Department temporarily stopped its BWC project simply because they were unable to respond to the number of FOIA demands. They ultimately solved the problem by recruiting the IT community to join in a so-called hackathon that provided a solution for efficiently redacting video before FOIA disclosure.[12] The financial impact is not trivial. In Berkeley, California, a small project that involved 150 cameras with only $50,000 in yearly storage costs was estimated to potentially cost the department about $1 million in lost productivity for the five full-time employee equivalents (FTEs) that were needed to administer and manage the collected video.[13]

---

[9] National Body-Worn Camera Toolkit, *Privacy*, U.S. Department of Justice, https://www.bja.gov/bwc/Topics-Privacy.html

[10] Ibid. 6.

[11] Justine Brown, *Oakland Police Test Cloud Storage for Body Camera Video*, Feb. 27, 2015, GovTech.com (division of e.Republic, Inc.), http://www.govtech.com/data/Oakland-Police-Test-Cloud-Storage-for-Body-Camera-Video.html

[12] Jennifer Sullivan, *Seattle police-hosted hackathon declared a success*, Dec. 19, 2014, Seattle Times, http://www.seattletimes.com/seattle-news/seattle-police-hosted-hackathon-declared-a-success/

Video analytics

Video analytics costs are currently the least understood program expenses, but they are potentially the most important in determining the true value and ROI of BWC video. Most recent BWC projects focused on the cameras and the static storage and management of video, with the necessary follow-up analysis that was performed either by the officer at the end of a shift or by investigators when the video becomes relevant to a case.

But this *view-it-as-needed* approach leaves much untapped potential value in those terabytes of video data. Valuable information can be left trapped in the system when human beings lack the time to uncover it. If no one is looking for something, it isn't found.

A higher value of BWC, and the approach that is recommended by the authors of this paper, is to make BWC video available for computer-based analytics to maximize its usefulness and minimize the human workload that is associated with video management. Only then will the true potential and value of BWCs be realized.

Finally, be aware that the video analytics field is buzzing with innovation, so adopting a platform that is closed to new analytic techniques can prevent an agency from realizing new investigative value from existing video content. Analytic techniques are likely to improve substantially during the useful life of the BWC equipment that is sold today (or over the life of the retained video).

BWC lifecycle

The U.S. Department of Justice, Bureau of Justice Assistance, developed what it calls the *National Body-Worn Camera Toolkit*, which offers implementation guidance for agencies that are interested in planning and adopting BWC programs.[14] The toolkit describes the need to establish policies across these primary BWC domains:

- Capture
- Viewing
- Use
- Release
- Storage
- Process and security

By using these domains as references, we created an eight-phase *BWC lifecycle*. See Figure 1 on page 7. Virtually every agency that uses BWCs will need to perform these activities, which are described in detail after the figure:

- Step 1. Record the video.
- Step 2. Upload the video for storage and archiving.
- Steps 3 - 7. Process the video for investigative or other purposes (multiple steps).
- Step 8. Release the video based on agency policies.

[13] Ibid. 6.
[14] National Body-Worn Camera Toolkit, U.S. Department of Justice, https://www.bja.gov/bwc/

Figure 1 shows the eight-phase BWC lifecycle.

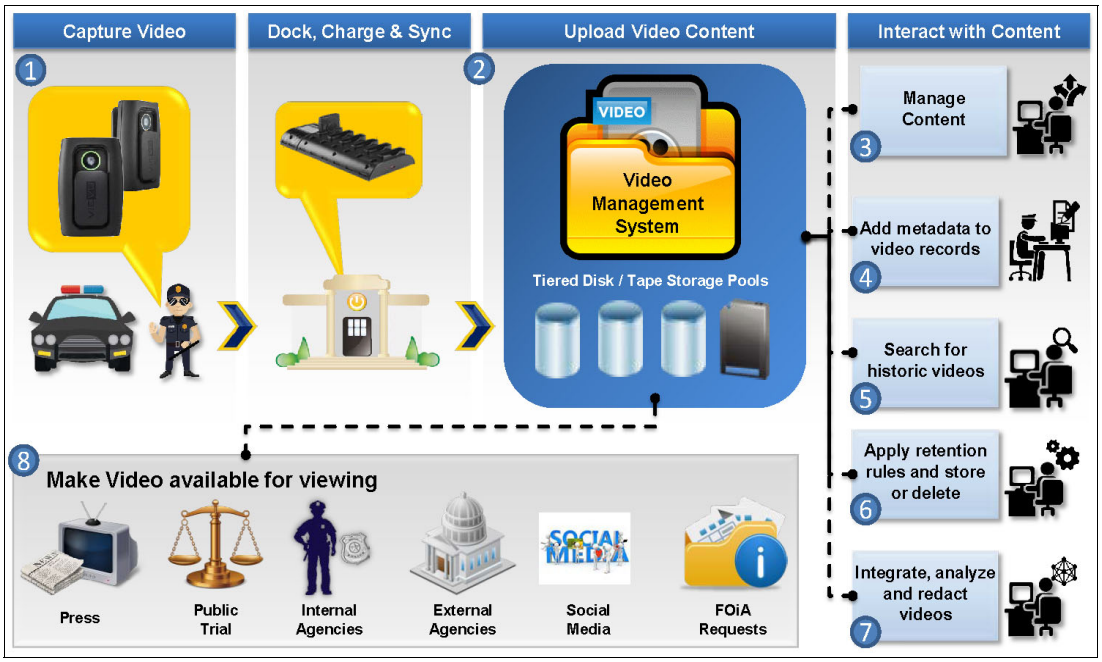

Figure 1 Phases of the BWC lifecycle

Thinking about BWC programs in terms of these phases can be useful when you adopt these programs and invest in the necessary IT infrastructure. When the phases are viewed this way, they become a virtual implementation plan.

Phase 1: Record the video

Capturing the raw video is an inherent, base function of the device that we do not address in this paper. However, video capture has its own set of challenges.

Police agencies need strong policies and procedures to define appropriate camera use by officers in the field, including the consideration of citizen privacy concerns. From an operational standpoint, the policies must also address considerations, such as when the camera is turned on and off in relation to when the particular incident begins and ends. This consideration not only affects aspects of the investigation but it also affects how much storage space is required. The Mesa, Arizona, Police Department employed two policies. One policy was restrictive and gave officers little choice about camera activation. The second policy was more discretionary. Officers averaged 2,327 video files each month while they followed the restrictive policy, and 1,353 video files each month with the discretionary policy, which represented a 42% decline in camera activations and an equivalent reduction in necessary storage.[15]

[15] Ibid. 9.

Phase 2: Upload the video for storage

The recorded video needs to be uploaded and ingested into a storage repository, which is typically a vendor-specific *video management system* (VMS). This upload is often performed when an officer returns from a shift and it can be accomplished either by placing the camera in a network-connected docking station or by using wifi. Almost all BWC vendors provide a way to upload video to either cloud-based or on-premises storage, although the methods can differ.

Several questions need to be considered in relation to video uploads and the related network requirements. Can the camera stream live video? If so, can it scale dynamic resolution to stream lower-resolution video (minimizing bandwidth requirements) while it still records the high-definition (HD) version to internal storage? Is video uploaded by using wifi? Will placing the camera in a docking station or cradle initiate an automatic upload? Can the camera switch between different upload modes?

Then, consider the issue of storage. Storage is always one of the most expensive components of BWC programs due to the volume of video and the varying retention requirements. Many options exist: cloud storage, on-premises storage (with tape or disk), or a hybrid of both. And costs are associated with each alternative. For example, consider the cost for basic cloud storage, and then add the amount the cloud provider charges for outbound data transfers. Simply placing files in the cloud is not the only answer. Certain agencies might not even accept cloud storage, and they demand on-premises solutions.

In either case, additional data security might be required. Agencies are also likely to be subject to security requirements in handling and storing BWC video content. In the US, the Criminal Justice Information Services (CJIS) division of the FBI is one example, with many agencies interpreting CJIS security standards to apply to cloud, as well as local storage.

Storing BWC content in a local data center has potential advantages:

- Fast access to video data and metadata to support special or emergency requests
- Local integration of the BWC application, content management, and storage solutions, leaving fewer variables to worry about
- Content access that is independent of Internet connectivity, which is subject to the provider's conditions or service terms and might result in insufficient bandwidth for certain use cases
- Local control of video access and chain-of-custody

Also, good reasons exist to locate storage in the cloud:

- Data is accessible from multiple locations, and it is maintained even if the local data center experiences an outage.
- Data storage costs are predominantly operational, independent of technology refresh issues and varying client IT skills.
- Cloud vendors might provide a contracted level of reliability and availability.

The cost for cloud storage for video must be evaluated closely. For smaller agencies with shorter retention policies, the cost of cloud storage might be manageable because the agency does not need to procure hardware, provide operations staff, and so on. For larger agencies or those agencies with longer retention policies, an on-premises or hybrid approach might be more cost-effective. In that case, initial retention can be on the cloud (or to both on premises and cloud simultaneously).

As the video ages, it can be transferred to more cost-effective on-premises solutions, such as linear tape systems. Keep in mind additional costs might be incurred to retrieve the video from the cloud. For long-term storage in the cloud to be cost-effective with large data volumes, a low-cost archive service is required.

In the end, we think most agencies will pursue lower-cost, on-premises storage to process local video and integrate that storage with a hybrid model that involves additional cloud storage. This approach maximizes operational efficiency while it minimizes costs.

Phase 3: Store and manage the content

The content repository is the primary, long-term storage area for BWC video. Management of the video content in the repository is important when the BWC program involves multiple camera vendors or when video content is spread across multiple VMSs. A robust *content management system* is an ideal add-on to a vendor-provided VMS.

The overarching content management system can be set up to assist with chain of custody procedures, evidentiary requirements and rules, integration with other, unstructured (non-video) content that relates to the case, and integration with multiple video sources (from other BWC vendors, dash-mounted cameras, citizen-captured video, and so on). The original video must be maintained even as new variants of it are created (such as to enhance the images or redact portions of the video). Ideally, the content management system must also be able to handle other forms of digital evidence, including still images, audio files, text reports, and investigators' notes, so that every digital asset that relates to the case is in a single system.

Phase 4: Add metadata (additional information)

Officers might need to add details that describe the content of the video and insert appropriate tags or other information that is not automatically captured, such as case numbers. Adding this information, which is called *metadata*, might sound fairly simple, but questions must be considered in this area, as well.

Who is authorized to add and edit these details? Can additional users be authorized to perform this work? Do these controls exist at all? More specifically, can new chapters be added to the video timeline? Can the video images themselves be annotated with comments or other pertinent information? Are other individuals, such as defendants' attorneys or other third parties, allowed any of these capabilities?

Tagging video provides the opportunity to integrate it with other agency systems. One tagging tool is IBM i2® COPLINK®, which can help a crime data warehouse ingest data from multiple sources, including records management systems, and search the data for tactical lead generation. Authorized personnel from multiple agencies can even search across COPLINK nodes.

All BWC vendors provide a means to *automatically* add metadata to videos. The basic functionality typically includes the insertion of dates, times, camera ID numbers, and possibly geo-location codes to identify where the video was captured. As BWC devices become smarter, more meta information will be available, for example, accelerometer data to show speed, compass data to show direction, and possibly even spoken-word transcription. Valuable insights can be gathered from this *extra* data.

Phase 5: Search the video repository

BWC systems usually include the ability to search for videos by date, case number, officer ID, metadata tags, and so on. Searches are performed during all phases of the evidentiary cycle, whether to respond to requests from a court, to respond to FOIA requests, or for basic file retention and backup. As the volume of stored video content grows, the efficiency of the search tools becomes a key usability factor. And in the future, police agencies will likely want the ability to search not merely on the video metadata but also audio transcripts of interactions and interrogations with suspects.

Phase 6: Retain the video based on established rules

In most jurisdictions, the rules are still poorly defined for how, and for how long, video content must be retained. We predict that BWC video will in most cases be classified as evidence. Therefore, agencies will need to retain most video for up to 20 years or possibly for the life of the involved parties (depending on local evidentiary regulations).

This need to retain videos for varying periods of time necessitates the development of retention rules. The cost of storing video means that agencies cannot retain *all* of the video forever. So, the rules must cover not only the duration of retention but also the circumstances, including when to know that a particular video recording has no further legal or regulatory reason to be retained. It is even likely that different retention rules apply to different portions of the same video based on the specific activities that are depicted.

Phase 7: Integrate, analyze, and redact the video as needed

Clearly, nearly all BWC video must be reviewed. This review enables you to integrate the videos with other videos from the same incident, review whether anything was captured on the video, and determine whether the video is worth saving. Videos will also sometimes need to be shortened. Portions of the video might need to be redacted. The cost for this work can be significant. But does a human being need to perform the review?

Video analytics tools can be used to pre-process video content and alert the correct personnel when certain recordings warrant further review or processing. This type of machine pre-processing can address many personnel, management, and financial issues. For example, a video that was thought to apply to only one case might, through analysis, be identified as containing evidence that relates to another, separate criminal case.

Phase 8: Release the video based on agency policies

Ultimately, BWC videos must be released for viewing by other individuals, whether they are directly involved in the case (police officers, prosecutors, defense attorneys, and so on) or are outside observers (such as the news media and members of the public).

Several questions exist within this realm. Who within the police agency is authorized to view the video, everyone or just those individuals that are directly involved in the case? What about the news media and the public (FOIA requests)? How are videos distributed? Must the videos contain the complete raw footage or can only redacted versions be released?

Considering the complexities that are involved in releasing videos correctly, we think a content management library for video and related files will soon be a necessary component of every BWC implementation.

IBM solution overview

The IBM approach to managing BWC programs starts with the belief that agencies need systems that can work with multiple types of BWCs, a wide variety of video sources (such as video that is taken by using smartphones or captured from surveillance cameras), and other kinds of unstructured content. This asset-agnostic approach avoids the cost of buying multiple systems to handle different types of content and makes it possible to use a single, unified user interface for adding metadata, searching videos, and viewing them. The combined approach even extends to video analytics software and content management systems, if the agency chooses to expand its BWC program into those areas.

The IBM approach also allows agencies that are implementing BWC programs to use equipment from multiple BWC vendors. We think it is highly unlikely that a single vendor will be able to meet all of an agency's BWC needs over many years (for example, undercover officers will likely need cameras that can be concealed easily, compared to uniformed officers who can wear cameras in the open). Figure 2 shows a high-level view of the proposed end-to-end IBM solution for BWC programs. After the figure, we explain the components of the solution in detail.

Note: Although the diagram depicts a hybrid solution with components that are deployed both in the cloud and on premises, any or all components can live totally on premises or be entirely cloud-based. Naturally, the option you select can change the funding basis for the solution (from cap-ex to op-ex or vice versa).

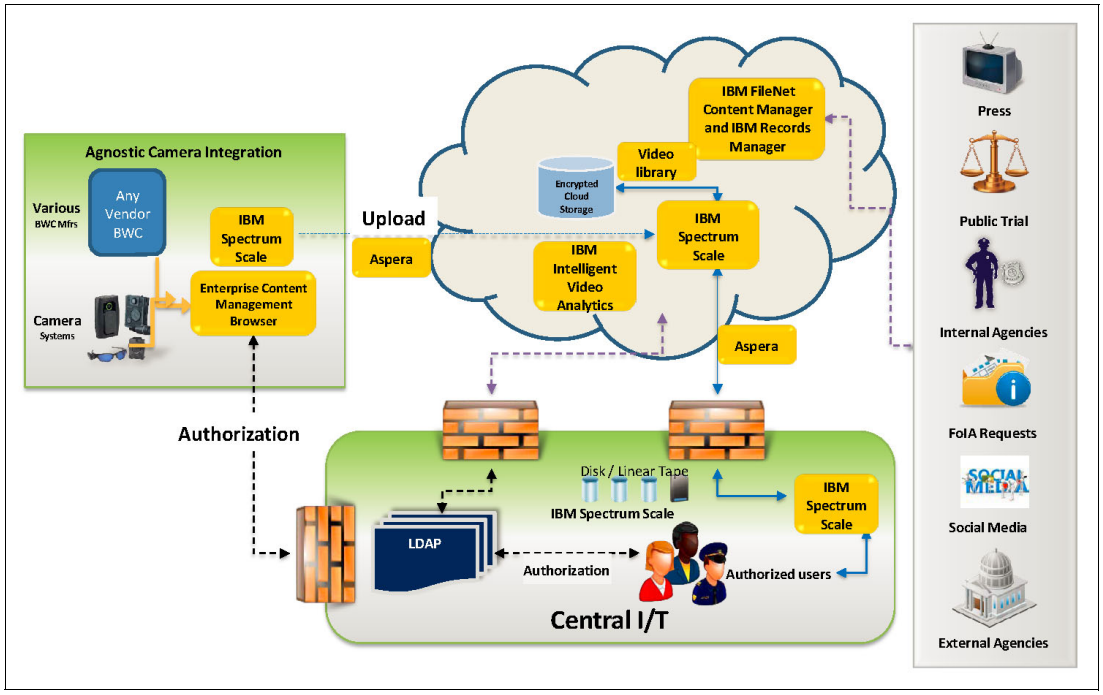

Figure 2 High-level view of the proposed IBM BWC solution

Solution components

We describe the major components of the IBM solution, the foundation of which is provided by components in the IBM Enterprise Content Management (ECM) portfolio. This paper does not specifically address the body camera devices or the process of recording BWC video because those operations are almost entirely controlled by the BWC vendor.

Content management/video repository

For content management, we recommend the use of *IBM FileNet® Content Manager* with video library functionality that is provided by a third party, such as Kaltura. FileNet Content Manager provides a unified user experience that can run on desktop computers, notebooks, and mobile devices. Most importantly, the video content is secured, processed, and maintained like any other content. This capability allows the agency to incorporate the video into other areas:

- Workflows
- Case management
- Collaboration and training programs
- Information lifecycle governance and retention
- Regulatory compliance
- Records management

In addition, the video navigator functionality that is provided by *Kaltura Video Navigator for IBM ECM* provides integration between the solution and the agency's video tools to add, update, search, publish, and watch videos across many devices.

After the video is in FileNet Content Manager, the video is treated like any other unstructured content. Thumbnail images are automatically generated for easy identification of each video asset. Retention and disposition rules can be enforced as defined by the organization. Access to the stored video is tightly controlled. The ECM system can designate the use of write-once-read-many (WORM) storage media for the appropriate content. The video itself can be previewed anywhere by using IBM Content Navigator, from any device with optimal quality, enabling secure and unified access anywhere, anytime, on any device. Viewing is optimized (regardless of format) for geography and device, with dynamic network bandwidth control that ensures that the video streams without buffering.

With FileNet Content Manager, agencies can add metadata to the videos, which allows the videos to be searched like other content. Spoken words in the video, if transcribed, show up in the search results, allowing video content to be accessed quickly and efficiently.

Records management

IBM Enterprise Records helps users address the evolving regulatory and legal requirements for BWC programs. Proactive adherence to information retention policies and procedures is critical. IBM records management products help organizations enforce centralized policy management, retention schedules, and legal preservation holds, and assists with audits, too.

IBM Enterprise Records works with ECM so that you can write and apply retention rules. For example, if the video is evidentiary, the video might be retained until the case is resolved, or, if the video is not evidentiary, it might be possible to delete the video after one year.

Automated video analytics and redaction

IBM Intelligent Video Analytics identifies events, attributes, or patterns of behavior through video analysis. IBM Intelligent Video Analytics is used for video surveillance but it can also be applied to BWCs.

Automated video analytics and redaction provide three key capabilities:

- Video tagging: Video tagging uses computer technology to identify interesting elements in a video and to provide metadata about those elements to use to help automate and accelerate searches of the video library. For example, video tagging can identify people in the video, what color clothes they are wearing, and their hair color. It can recognize vehicles, even differentiating between trucks and sedans and their colors. Video tagging can also identify specific actions, such as pointing a gun.
- Video redaction: Video redaction is an important feature for BWC video that is captured outside of controlled circumstances, such as in public places. Video redaction allows for removing or blurring parts of a video with minimal human interaction, identifying people and other objects that must be obscured before the video is released.
- Facial (or other) recognition: The ability to recognize faces or other objects (such as particular types of vehicles) within a video also is an inherently important function that enables the possible identification of objects that a human being might not see, or that can take a prohibitively long time for a human being to identify.

Transfer and storage options

BWC videos are uploaded and eventually stored in a form of physical storage.

Transfer

Uploading requires high-speed, large volume file transfer capabilities, but video files are large and transferring them across a network can create bottlenecks. One way to alleviate these bottlenecks is with *IBM Aspera*®, which is a high-speed file transfer solution that integrates with mobile devices, cloud systems, and on-premises repositories.

The Aspera patented IBM Fast Adaptive Security Protocol (FASP®) transfer technology eliminates the largest shortcomings of conventional, Transmission Control Protocol (TCP)-based file transfer technologies. FASP transfers can be hundreds of times faster than FTP and HTTP and provide predictable delivery times regardless of file size, transfer distance, or network conditions. Security tools, including secure endpoint authentication and dynamic or immediate data encryption, are built into the product.

Aspera also supports streaming video solutions that eliminate the need to dock the BWC device for uploading. Naturally, the network impact must be evaluated when you consider any form of network upload or streaming.

On-premises storage

Law enforcement agencies will amass a tremendous amount of video content, part of which is subject to ongoing access, while they preserve the rest for evidentiary and regulatory compliance. The choice of storage in a BWC solution involves three key decisions:

- Support for access patterns and certain retention policies
- Choice of storage media, especially for long-term retention
- Location of the data storage (Will it be on premises, in the cloud, or a combination?)

Storage access patterns will vary over the lifecycle of the video content. Uploading, ingestion, analytics, and redaction all require intensive access to the video content. Access to certain content will be sporadic over a defined period (for example, six months), as its evidentiary status changes. Content that becomes evidence eventually has long-term retention requirements where the probability of access is low. This kind of content must be stored at a low cost. However, content with *no* evidentiary value needs to be deleted in a defined time frame.

The core of the IBM storage solution (whether the solution is on premises, in the cloud, or a hybrid of both) is *IBM Elastic Storage Server* (ESS), which is software-defined storage that uses IBM Spectrum Scale. ESS links with video lifecycle management tools to use multiple tiers of storage (based on the lifecycle stage) while it optimizes the cost of storage as usage scales up and as technology must be refreshed.

ESS can transparently migrate data among pools of storage media without requiring downtime or outages. The ESS policy engine can automatically maintain content on the media that best matches its access requirements and status in the evidence lifecycle. ESS uses fast-access solid-state storage and variable-density spinning disk for access within microseconds or milliseconds.

For content with the longest retention requirements, integration between ESS and *IBM Spectrum Archive*™ uses the IBM Linear Tape File System (LTFS) to archive data in a vendor-neutral Linear Tape Open (LTO) format. Files on LTFS tapes can be accessed directly without backup/restore or archiving software. In addition to high-density tape cartridges, WORM tape cartridges go beyond software controls to protect against the change or removal of important evidence. Metadata for archived content remains quickly and locally accessible to assist searches and lifecycle operations, while the archived video content is stored at the lowest possible cost and highest possible density.

Therefore, storing content in the local data center has the advantage of faster access, tight integration with content management, and local access control. However, cloud storage also has potential advantages. Content in a cloud is accessible from multiple locations in a local outage. Content in a cloud might benefit from contracted service levels and economy of scale, and its cost is predominantly operational.

Anticipated future developments for BWC programs

The BWC solution space changes rapidly. We see three technology themes that might become part of the BWC landscape soon.

Video streaming

Most BWC implementations currently use a form of docking or wifi technology to upload video. However, streaming video might become more pervasive soon. Streaming offers several potential benefits:

- Seeing events unfold live
- Reducing end-of-shift burden (both on LEOs and the BWC network)
- Real-time alerts and notifications, such as informing a central system when a BWC is turned on

One consideration will be what gets streamed from the device and when. Streaming video from multiple devices continuously will likely be too expensive for many police departments, especially if that data must comply with CJIS standards that require private transmission and storage and the use of dedicated video processing equipment. Today, experts are investigating a number of options that, individually or together, might help police agencies manage the volume of video that will be streamed:

- Varying the resolution of the images
- Using video sampling and transmitting, for example, only every 10th frame (except when events require more frames)
- Omitting aspects of each image that are not relevant to the action that is viewed (analogous to how the MP3 standard compresses music transmissions)
- Storing videos on the camera for short periods and then forwarding the videos as bandwidth becomes available

Ultimately, the selected methods will reflect the balance that the police agency wants to strike across the realms of cost, accountability, and the protection of officers and the public. We anticipate that BWC vendors will want to help agencies make these choices by, for example, including analytics capabilities in their devices to automatically adjust frame rates and resolution in response to what the camera sees.

Clustering crowdsourced videos (with live streaming)

Another promising capability is combining multiple video streams and enabling multiple angles and views of the same event. An IBM research project that is called Clustering crowdsourced videos[16] envisions video-sharing services for live user video streams. This technology can likely be applied to BWC programs.

BWC videos capture the unique perspective of the observer, which might miss other valuable views that can be captured from different angles or vantage points. Unfortunately, due to the multitude of possible sources, this video content is difficult to browse and search. Approaches to organize these multi-angled views were attempted before, and they typically rely on a haphazard index of user-provided tags and comments. And although tags and comments are useful, they require manual effort, might not be descriptive enough, are subject to human error, and might not be provided in real time. Therefore, tags and comments are not amenable to live video streams.

In contrast, the IBM research team envisions a real-time system to extract content-specific metadata for live video. This idea is to deduce content similarity even when videos are taken from dramatically different perspectives. For example, when officers at an accident film the vehicles from different locations on the street, each officer might capture a distinct background. The shared foreground vehicle will appear substantially different from the different angles. Human interaction is typically required to discern the similarity. However, the sharing solution that is now being developed can discern the similarity automatically.

[16] *FOCUS: Clustering Crowdsourced Videos by Line-of-Sight*, http://slidegur.com/doc/128065/focus--clustering-crowdsourced-videos-by-line-of-sight

The Internet of Things

A paradox of the Internet of Things (IoT) is that ultimately, the value that the IoT adds is not about the *things* themselves. The value lies in the insights that are derived from monitoring the things, which can then be applied to real-world problems and situations. Therefore, the *things* (in this case, BWCs) are ultimately merely commodities. They are another device that captures data. The IoT has several implications.

BWC vendors, like vendors of sensors in other contexts, will attempt to resist the commoditization of their devices by adding intelligence to them. Examples might include geotagging, image recognition, and the ability to switch camera capabilities (for example, if a camera has an external screen, the camera can be turned off at night to prevent suspects from seeing an officer approaching). Agencies are also interested in integrating BWC data with data from other sources, such as gunfire-detection systems or vital-signs detection systems for police officers.

IBM can help with the IBM Internet of Things Foundation. The Internet of Things (IoT) Foundation is a fully managed, cloud-hosted service that makes it simple to derive value from IoT devices. With the IoT Foundation, you can collect and manage a time-series view of data and see what is happening on your devices in near-real time, and store your IoT device data in a database for analysis.

Next steps

A BWC implementation includes much more than evaluating, procuring, and implementing the devices. First, conduct a thoughtful planning process that involves various stakeholders to establish the critical policies and procedures under which the program will operate. The plan must also include a communication and education campaign for all stakeholders.

As policies are better understood and the camera technology is reviewed and tested, additional technical considerations will need to be addressed. These considerations are part of the BWC lifecycle that was explained earlier. The following considerations are important:

- Evaluate the need for a content platform. Rather than selecting one vendor or a closed architecture, adopt an approach that will support multiple vendors and cameras. After all, will the initial choice be the choice forever? Will only a single camera solution be mandated?
- Estimate the expected storage costs by using assumptions about the adoption of specific BWC technologies, the retention of content, and the trends in body camera equipment. Include factors, such as network bandwidth and the cost of cloud access and downloads.
- Evaluate solutions that can minimize the human costs. These costs can be lessened by using video analytics and redaction, facial recognition tools, and search capabilities. Consider a platform in which analytics capabilities can be added incrementally as new technology becomes available.
- Evaluate the need for an automated method to adhere to video retention rules. Storage costs can be reduced and managed and policies can be more easily followed with a solution that includes automated records retention.
- Evaluate the need for a common content management solution at the back end to allow the integration of multiple video sources with other unstructured content.

How IBM can help

The IBM platform provides maximum flexibility and cost-effectiveness for agencies that are implementing BWC programs. The IBM approach is anchored around four key tenets:

- Provide a complete end-to-end platform to address all of the steps of a BWC lifecycle.
- Provide maximum flexibility and *future proofing* by providing the capability to integrate with various video sources (including cameras from multiple vendors, dashcams, smartphones, and so on) and other unstructured content.
- Base the solution components on what we learned as an innovator of complex content and video systems, and use leading-edge tools for analytics, facial recognition, real-time video streaming and analysis, and more.
- Design a cost-effective storage environment that balances cost-effectiveness with easy and timely retrieval of video content.

The BWC market grew tremendously over the past few years with new products and new players regularly surfacing. In addition to staying abreast of the fast pace of technological change, law enforcement agencies must address what is expected to be a shifting landscape of standards, protocols, and policies. The solution that they adopt must remain relevant and keep pace with technological and policy changes.

The ideal BWC *solution* is a solution that can readily embrace new technological advancements. The ideal BWC *end-to-end provider* is a provider, such as IBM, that can work with its clients to adapt to emerging protocols.

Resources

The following resources offer more information:

- IBM FileNet Content Manager

  http://ibm.co/1O7T8ai
- IBM Enterprise Records

  http://ibm.co/1W7zNv7
- IBM Intelligent Video Analytics

  http://ibm.co/1OwvOXr
- IBM Spectrum Archive and LTFS tape

  http://ibm.co/1kazv4b
- IBM Elastic Storage Server with Spectrum Scale technology

  http://ibm.co/1PJXA3w
- Kaltura Video Navigator for ECM

  http://ibm.co/1OMHuBa
- IBM IoT Foundation

  http://ibm.co/1L1WkE1

About the authors

This document was written by these IBM experts.

Richard Budel is a member of the IBM global public safety team. Richard is a former civil servant with decades of experience across the world and numerous publications about the topics of the public safety lifecycle and ROI for public safety spending.

Peter Coldicott is a member of the IBM Academy of Technology and an IBM Distinguished Engineer. Peter is the CTO for the IBM Safer Planet Division software development organization, which includes responsibility for IBM software solutions for Law Enforcement, Emergency Management, Counter Fraud, and the Intelligence community.

Steve Correl is a Senior Managing Consultant, IBM Systems Lab Services. Steve works with clients across industry segments on large-scale hybrid cloud and data storage architectures.

Don Dejewski is a member of the IBM Academy of Technology and an IBM Executive Architect and a Technical Advisor to public sector clients. Don designed many solutions for State and Local and Public Safety clients.

Mark Dixon is a member of the IBM Academy of Technology and an Executive Architect for IBM Smarter Cities® and Safer Planet solutions. Mark designed solutions for Commercial, State and Local, and Public Safety clients.

Peter Williams is a member of the IBM Academy of Technology, an IBM Distinguished Engineer, and the CTO for Big Green Innovations.

The paper was produced with the International Technical Support Organization (ITSO), Poughkeepsie and Raleigh Centers. **Shawn Tooley**, Technical Writer, ITSO Raleigh, contributed to the production of the paper.

The authors thank the following additional people and groups for their contributions to this document:

- Trinette Brownhill
- Thom Garcia
- Peter Guglielmino
- Jan den Hartog
- Bill Josko
- Hung Tack Kwan
- Alison Oleksiak
- Denis Tsai
- Greg Wallace
- The IBM Academy of Technology

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and client satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online:

http://www.ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:

  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm
- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document REDP-5276-00 was created or updated on January 13, 2016.

Send us your comments in one of the following ways:
- Use the online **Contact us** review Redbooks form found at:
  ibm.com/redbooks
- Send your comments in an email to:
  redbooks@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks

REDP-5276-00

ISBN 0738454931

Printed in U.S.A.