White Paper

Video Surveillance Storage

Understanding the Body Camera Video Surveillance Storage Considerations

By Dan Conde, ESG Analyst

October 2016

This ESG White Paper was commissioned by Dell EMC and is distributed under license from ESG.

Contents

Introduction

With increasing volumes of video evidence, law enforcement agencies need to understand the tradeoffs involved in making decisions that can resonate over many years. It is apparent that law enforcement agencies are now storing more video evidence from body cams, drones, in-car video cameras, and crime scenes. With so much video data being created, it has become a challenge to understand how best to address the needs of law enforcement, comply with legal requirements, and address costs and convenience at the same time.

Challenges

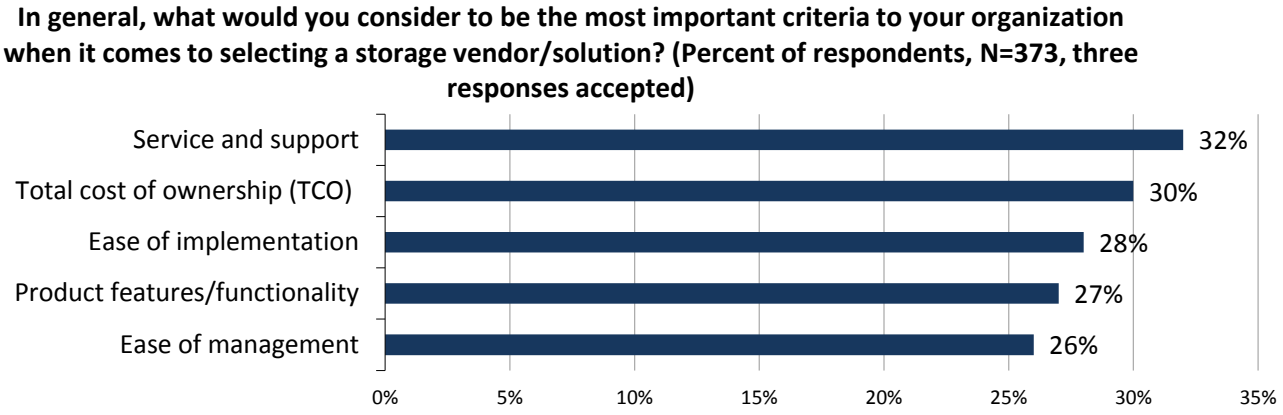
Large-scale deployment of body cameras is still a relatively recent development for most law enforcement agencies. Although it is convenient to start using the cloud-based storage provided by the video camera vendors, it is important to understand the long-term implications of doing so for law enforcement and IT. Storage of body camera video evidence is different than storage of regular files, email, or even regular photographic evidence. Evidence cannot be easily stored in the cloud, like email and word processing can, due to regulatory compliance requirements such as data sovereignty. Hybrid or on-premises storage uses will help address the range of these requirements related to location. Silos of video information from different sources reduce collaboration unless they are combined into a shared surveillance data lake.

Considerations

There are many considerations when adopting a solution for storing video surveillance and evidence data collected from devices such as body-worn cameras. It is important to understand the concerns for IT organizations and for the broader set of law enforcement agencies evaluating storage.

What criteria do IT decision makers consider when evaluating storage solutions or vendors? In 2015, ESG conducted a research study investigating the general storage industry that surveyed 373 IT decision makers. Respondents were asked to identify their organizations' most important criteria for selecting a storage vendor or solution. While technical features are important, the two items most-often cited by respondents were related to business issues: service and support as well as total cost of ownership. This demonstrates that organizations are willing to make up-front investments in order to increase efficiency and cost savings in the long term.[1]

Figure 1. Top Five Criteria for Selecting a Storage Vendor/Solution



Source: Enterprise Strategy Group, 2016

[1] Source: ESG Research Report, *2015 Data Storage Market Trends*, October 2015.

Cost

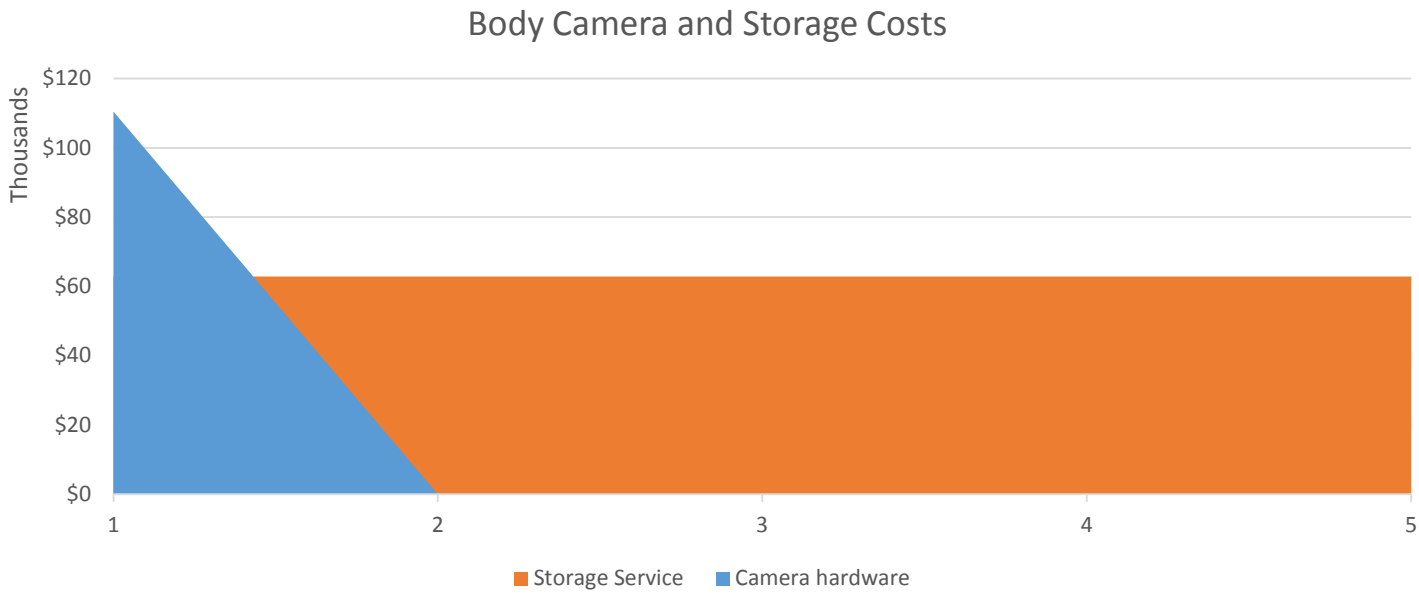
Cost is a critical concern for government agencies, and some cloud storage plans that offer unlimited storage as part of a subscription service may seem advantageous. After all, if one cannot predict the volume of camera evidence to be collected, an unlimited storage solution seems tempting: Costs for storage will be predictable, and overage fees will not exist.

However, for the same reason, an "all you can eat buffet" of unlimited storage subscription services may not be the right solution. There are many issues to consider before adopting an unlimited storage plan. For example, the capacity of storage one actually needs will be less than the size of the full video recording captured because unnecessary footage will be redacted before storage. Unlike saving all snapshots for home videos or photography, there are more careful considerations for storing evidence.

Therefore, on the basis of cost per storage capacity, the unlimited plan may turn out to be more expensive than necessary, and the advantages of an unlimited storage plan may not materialize. Furthermore, in order to benefit from an unlimited storage plan, organizations may need to sign for a five-year contract, which could result in a high total cost of ownership.

A body camera could cost about $500 on average, but the storage may cost $70 to $100 per camera per month, not including maintenance and replacement costs. As an example, over the five-year contract for the police department in the city of Alameda in California, $424,753 is the total cost of purchase over five years for both equipment and media storage as disclosed in 2015. The first year fee for equipment and storage is $173,329, and media storage for the second through fifth years is $62,856. Thus $110,473 (26%) is allocated to the equipment (the body cameras themselves) and the remaining $314,280 (74%) is for media storage (see Figure 2). Thus the total data storage costs for outfitting police officers may be significant for organizations using a public cloud infrastructure. This allocation may surprise those who focus solely on the hardware. This is similar to mobile phones, where the attention is paid to the device, but over the years, the service plan costs comprise the significant portion of the overall costs.

Figure 2. Components of a Combined Five-year Contract for Body Camera and Storage Service (80 Officers)



Source: Enterprise Strategy Group, 2016

Thus one may consider an alternative plan—paying only for the capacity of the cloud storage used. That seems fair, since the cost tracks actual usage. Organizations may run into a problem with this plan, however, since costs for cloud storage are fixed on a per-megabyte basis. In practice, there is a difference in types of evidence—current evidence for cases under investigation is treated differently than archived evidence. Just as old physical evidence is eventually moved to a remote archival facility, it does not make financial sense to pay for archival video storage in the same manner as evidence needed for current and ongoing cases. Different methods of video storage are required based on how important the data is. This is an issue of exerting better control over the type of evidence to store, and assigning it the right cost.

In practice, the cameras are upgraded every two and a half years and the upgrade costs are included in some cloud provider contracts. Therefore, there is a hidden camera upgrade cost in the media storage cost.

Later in the paper, we examine how costs are allocated between the cameras and storage. The important consideration is that camera costs are a minor part of the total outlay. Storage media costs are the largest part of the costs, so controlling storage goes a long way toward controlling the total body-worn video program costs.

Integrated Storage Platform

In addition to body cameras, law enforcement agencies need to store data from a variety of sources, such as videos from crime scene stationary cameras, drones, interrogation room cameras, and law enforcement vehicle cameras, as well as photographs from cameras. The data needs to be stored and managed in a consistent way, with common compliance requirements and procedures for access and workflow. If an organization already has existing processes and software for searching, providing access, and redacting evidence, it makes sense for body camera evidence to fit into those processes. There is little reason to treat body camera video data separately just because the camera vendor provides an integrated storage service.

Local Storage and Control

The simplicity of cloud-based body camera storage is ostensibly appealing. It does not require extensive equipment, and perhaps all an organization needs to do is deploy a charging station for each camera that also serves as a data-upload dock, connected to the network.

However, unless the organization is converting all evidence storage to the cloud, the existing evidence storage infrastructure will still have to be maintained. The law enforcement department will continue to collect evidence from many existing sources, including standard photographs and traditional video footage, and it only makes sense to keep all of the collected evidence in the same location and treat it in the same manner.

Unlike cloud-based storage, utilizing storage under direct departmental ownership and management will provide organizations with better control over evidence, and a means for applying appropriately priced storage to the different types of evidence.

With control over their storage design, organizations can choose to back up and archive old evidence to cheaper storage. This can provide savings as they store more evidence. Compare this with cloud storage, where one pays based on a single cost structure for all forms of evidence.

Local storage of video evidence may provide a better experience for capturing videos, since the equipment is directly available at the police station and does not require access to the cloud via an Internet connection for uploads. Similarly, locally stored video evidence will be available for faster retrieval and analysis.

Management and Collaboration

Video evidence storage is not simply a matter of storing and retrieving the data, like one would with paper files in a filing cabinet. Law enforcement agencies will need to share and actively use the stored evidence. This is why using nonproprietary video formats is also important since data needs to be exported to different systems and organizations. The value of the data comes from managing it and collaborating with a group of people in a workload to understand and extract value from the content. These goals are embodied in the standard operating procedures (SOPs) for digital forensic data. SOPs do not specify particular products or technology and are meant to be general guidelines. However, when implementing SOPs, each department establishes specific technical management procedures to make the management of video recordings comply with the SOPs.

For example, SOPs can be created based on policy recommendations in the U.S. Department of Justice Community Oriented Policing Services (COPS) recommendations (COPS-P296),[2] followed by appropriate implementation strategies such as:

- Agencies must protect the integrity and security of the video recording footage. An appropriate strategy for implementation is to use data storage systems with built-in audit trails requiring supervisors, and not the police officer, to download the recordings in which a police officer was involved. This helps ensure that data tampering, deletion, and copying are not allowed.
- Officers should properly categorize video recordings at the time of downloading. This may be implemented using an agency's existing record management system.
- Policies should clearly state where video footage is stored. Considerations include security, backups, long-term storage, and chain of custody, which leads to implementation tips that require consultation with prosecutors and legal advisors on chain of custody.

These policies indicate that procedures for video evidence cannot be performed in isolation, and are done in concert with record management systems and audit processes.

Similarly, video evidence is leveraged in concert with other forms of evidence, which are likely managed with existing infrastructure, and must comply with the same rules as the other forms, such as those dictating the release of information to the public. Essentially, the various forms of evidence and how they are handled must be integrated in a comprehensive manner, which will likely involve considering how video data can be incorporated into an organization's existing infrastructure with a well-defined and understandable process. Otherwise, bolted-on cloud procedures will disrupt the evidence process, potentially resulting in critical errors in law enforcement.

Many agencies are looking to hybrid storage systems, which combine public cloud and on-premises options, for the flexibility they need to integrate cloud-based systems with existing processes.

Skills

Storage of evidence is not simply an issue of hardware and IT infrastructure. It also requires the skills and training of the IT staff and law enforcement officers. Organizations have already invested in IT infrastructure and relevant training, so body cameras ought to be an incremental addition that leverages that existing training. Two parallel procedures—one for the traditional evidence and another one for the new cloud-based evidence—can lead to redundancies and complications.

[2] "Implementing a Body-Worn Camera Program," United States Department of Justice Product ID: COPS-P296, Published 9/9/2014, Authors: Lindsay Miller, Jessica Toliver, Police Executive Research Forum.

Regulatory Compliance

Evidence storage for law enforcement will require considerations for compliance with legal requirements. This includes Criminal Justice Information Services (CJIS) requirements, security required by the local jurisdiction, and high-level data sovereignty issues at the national level. For some countries, the data needs to be stored in the same country as the police force's jurisdiction. Categorization for evidence is also strict, and sometimes an act of a national and state legislature changes the importance of categories and required retention periods. For example, the state of California raised the storage requirements for general video evidence from one to two years, and this decision affects storage requirements significantly (California Government code 34090).

When an organization uses the cloud, where is the data stored? The answer to this question may be critical to understanding the implications of using cloud storage. A cloud storage provider needs to comply with CJIS requirements and although some providers are compliant, an independent solution provider may construct its own cloud backup system in other cases. In that case, it is important to determine whether the custom-built solution meets CJIS requirements.

Security for custom-built solutions is important as well. It is conceivable for an improperly secured cloud-based evidence storage system to leak un-redacted videos over the Internet, creating a publicity problem or, worse yet, affecting an on-going investigation or trial.

Law enforcement evidence also requires a strict understanding of the chain of custody. Once evidence data is moved to the cloud, how can an organization reliably ensure and prove the chain of custody related to that evidence? Even if a cloud provider offers some encryption capabilities to reduce tampering, moving data out of the agency's control means it is open to potential unintended disclosure or loss of access. Cloud storage may offer digital signatures to assist in the chain of custody, but that adds another process that may insert management complexity if the law enforcement agency already follows its own internal processes to protect the chain of custody.

Evidence Lifecycle Management

The difference between storing video evidence and storing other types of data in consumer-style cloud storage is that evidence needs to be kept for a long time, potentially up to 25 years or more. Thus organizations need to understand that new forms of cloud storage for video evidence, while initially appealing, are still novel and untested. It is not possible at this point to predict exactly how this storage can be relied upon to provide evidence many years from now. In the future, cloud storage may become the norm, but it is not certain what form it will take. It may be run by a consortium of law enforcement agencies and may not even be in the form of a private enterprise.

Evidence storage is different from many other types of storage in that most of it remains unused, by design. But once it is used, it becomes important and the data will be actively examined. In addition, video evidence data is not like an archival read-only document sitting in storage. Organizations can perform analysis on video, such as running facial recognition on the bystanders in the video, redacting information, and tagging the video images. Applying the same criteria for choosing cloud-based archival data storage for video evidence may not be appropriate.

Storing Data under Control

These considerations ultimately revolve around the issue of control. Losing adequate control over any kind of evidence potentially has cascading effects on compliance. Entrusting evidence to an outside entity reduces the level of control available to law enforcement agencies, which is important in the long term. Using an outside provider for storage reduces control over the management and collaboration processes already put in place by the organizations themselves.

Control is not directly related to the storage location—whether storage is located on-premises or in an off-premises cloud storage facility. Control is an advantage that organizations gain by providing appropriate decision-making ability over how the solution is managed and maintained.

Several options for cloud-based storage ensure that organizations maintain adequate control. One is a conventional on-premises storage system within the law enforcement agency's IT department. Alternatively, the IT department may create its own cloud service to provide the ease of access of cloud storage combined with the necessary level of administrative control. It is also possible to create a cloud-based evidence storage system for interdepartmental sharing at the county or even the state level. This kind of system will preserve control and provide the possibility of integrating existing evidence storage with body camera video storage. Entrusting video evidence to an external equipment vendor may lose the level of control necessary for law enforcement.

Dell EMC's Elastic Cloud Storage (ECS)

It is worthwhile for law enforcement agencies to examine a storage solution that addresses their specific needs. Dell EMC's Elastic Cloud Storage (ECS) is such a storage solution that offers many capabilities appropriate for video evidence storage. It is a solution that meets the needs of law enforcement agencies for on-premises storage, as well as for service providers creating an evidence storage system on behalf of law enforcement agencies.

By providing the option of a storage system that may be deployed on-premises or by a service provider to create a cloud service purpose-built for video evidence storage, ECS offers the appropriate level of control required by law enforcement, with the following capabilities:

- **Multi-purpose.** The ECS software-defined architecture supports many protocols and data formats, so it may be used for not only body camera video evidence storage, but also for other digital data, acting as a platform for traditional and modern application workloads. This addresses the integration requirements to interoperate with the workflow for other evidence.
- **Accessible.** ECS supports enhanced metadata search to enable rapid retrieval of the correct data. Its compatibility with common cloud APIs for storage means it enables the use of applications that leverage cloud protocols and provides the underpinnings to create an interoperable video evidence cloud storage system that can be provided by a service provider yet still remain very much under a law enforcement agency's control as an alternative to public cloud storage. This is an issue that will be increasingly important as on-premises systems need to be integrated with other software that may be designed for cloud, creating a hybrid solution.
- **Cost-effective.** ECS leverages commodity hardware as its underpinnings in order to lower total cost of ownership, and it can provide a lower TCO than public cloud and other object storage. This addresses traditional IT needs since body camera video needs to work alongside other IT assets under the same budget.
- **Enterprise-class.** ECS is supported by a leading storage vendor and meets storage compliance requirements.
- **Scalable.** ECS is based on a next-generation object-based storage system that supports geo-distributed data. It supports universal access to a variety of data formats, making it a platform for modern applications with increasing data needs.

Cost Comparison

A cost comparison of an ECS-based solution with a cloud based storage system from a popular body camera provider indicates that deploying on-premises storage is cost effective compared with using a cloud-based system. ECS Generation 2 Model U400T providing 640 TB of raw storage is used for comparison.

The assumption:

- Police department is supporting the use of 100 cameras. Cameras may be shared between officers, so we assume two shifts per camera. Three shifts are not chosen in order to provide sufficient time for extracting the video data and recharging.
- Video resolution is high definition, with MPEG-4 AVCHD/H.264 generating 6 Mbps. Data generated ranges from 2.7 GB per hour at 15 frames per second to 5 GB per hour at 30 frames per second. We will use the 2.7GB estimate. Data rates will vary depending on the scene.
- Each eight-hour shift generates one and a half hours of video.
- Video is stored for 24-month retention and 1% of permanent hold retention for evidentiary data. The retention period is a conservative choice on the upper end of the scale required by agencies.
- Each shift generates 4 GB of video per day. At 24-month retention with 30 days of duty per month creates 5,760 GB of video data per camera under dual shift use.
- One hundred cameras each used in two shifts results in 576 TB per use, which fits into the 640 TB of ECS storage, with excess storage reserved for 1% evidentiary video to be stored after the retention period allows deletion.

For purposes of comparison, we calculate cost per camera. Comparison is based on ECS hardware and cloud provider contract.

- ECS: The list price is $266,980 for the hardware, with an additional $24,028 based on 9% per year for enhanced-level maintenance, resulting in a total cost of $387,121 over five years for hardware and maintenance. For storage, this is equivalent to $65 per camera per month in a 100-camera fleet.
- Cloud provider: The list price is $79 per user per month for its unlimited plan, which is $94,800 per year resulting in $474,000 for five years for 100 cameras, including one camera upgrade.
- Camera upgrades under ECS: Over the five-year cycle, the cloud provider plan provides for a camera upgrade each two and a half years. In the ECS plan, we will add $500 for a camera upgrade, raising the total cost by $50,000. This is added to the ECS storage cost, which results in a total cost of $437,121, making the camera and storage combination with ECS cost $73 per camera per month. Note that under the ECS plan, there is freedom to choose any vendor for the camera without being locked into a particular brand.

The cloud provider plan includes software services such as reporting, redaction, and data management. It may be necessary to add costs for video management software for ECS costs, and backup or archival software and media to store non-current data; however, if the organization has on-premises storage for traditional video evidence, it may already possess such software for management or redaction.

Since a video camera is used in either on-premises or cloud-based, the initial camera hardware costs are taken out of the comparison since the storage costs comprise the majority of the costs. However, cloud provider pricing may include some costs allocated to camera upgrades and in some plans, for payment toward equipment. To enable a better comparison, we upgraded the camera under the ECS scenario.

Although the cloud provider offers a lower cost subscription plan, this is not a practical route since the storage is limited to 10 to 40 GB, which may be depleted under common usage scenarios. Unlimited storage from the cloud provider provides predictability in pricing, but it is limited to storing the contracted camera uploads, and additional storage costs 6.25 cents per GB per month for photographs or dash camera videos. Therefore, either other forms of storage are necessary or additional costs need to be budgeted.

Under this scenario, cloud provider costs are $4,740 for five years, at $2.19 per GB for storing video for the first year. By comparison, ECS provides a 640TB pool of storage shared among all police officers, and the cost is $0.59 per GB of raw capacity over five years.

The initial outlay for ECS is higher since it entails an initial equipment purchase, but the costs do not increase over time, other than paying for maintenance. The equipment will need to be eventually refreshed, but that depends on each buyer's refresh schedule. The initial costs are amortized over the entire period so the longer the ECS storage is kept, the equivalent monthly cost per camera declines.

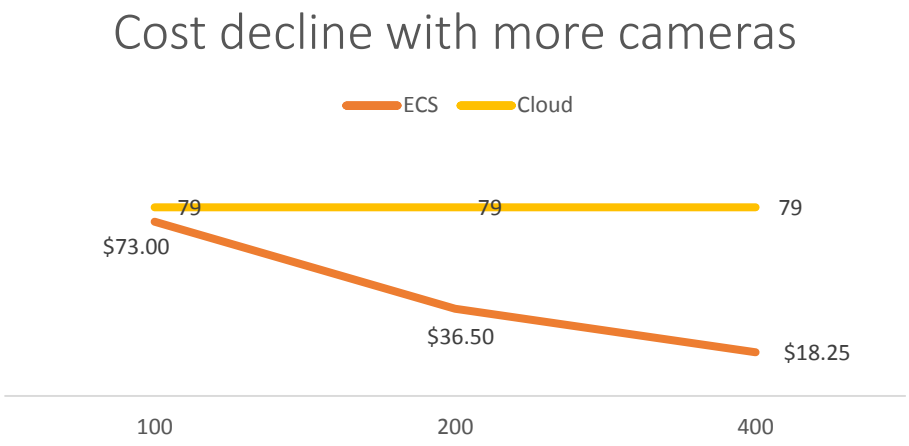
The question is how the storage capacity from either ECS or the cloud provider will be used over a period of five, ten, or 15 years. This depends on the rate of redaction of videos, whether new cameras generate more data, whether officers record more footage per shift, how retention policies change, and whether videos from on-premises storage are archived to offline media.

Without any redaction, ECS storage will run out of capacity while an unlimited cloud provider retains the same costs, provided it retained a fixed-price contract. There are two methods for controlling storage on-premises. One is offline archival backup, which may be augmented by the redaction of videos. The second is redaction that may be done manually or by automated systems.

If the on-premises storage is sufficient for storing the camera videos for four to five years, then the cost benefits of ECS outweigh the unlimited storage of cloud providers. In addition, there are issues related to control as mentioned earlier that favor on-premises storage.

The process for redaction depends on the policies of each law enforcement agency, such as the minimum retention polices. Evidentiary data needs to be stored as long as the court case is relevant or as required by state law. Non-evidentiary video retention policies range from "unspecified" through 45 days in Charlotte, NC to two years in Oakland, CA. Given this variation, it is difficult to construct a single model for retention, but it is safe to recommend that evidentiary data be kept online on on-premises storage such as ECS, and that other data be archived on backup media. The comparison was conservative in choosing a two-year retention period. If a shorter period is required, then the ECS system can store media for more cameras, or a lower cost storage system may be purchased. We show how the cost per camera declines as more cameras are accommodated by an ECS system with a shorter retention period in Figure 3.

Figure 3. Cost Decline with More Cameras



Source: Enterprise Strategy Group, 2016

Choosing a platform for video storage is not a simple issue of cloud versus on-premises. This paper's analysis is not meant to present a "pro on-premises" perspective. Even if costs favor on-premises, issues related to convenience may dictate the use of some cloud storage since some remote law enforcement officers find it convenient to use cloud storage.

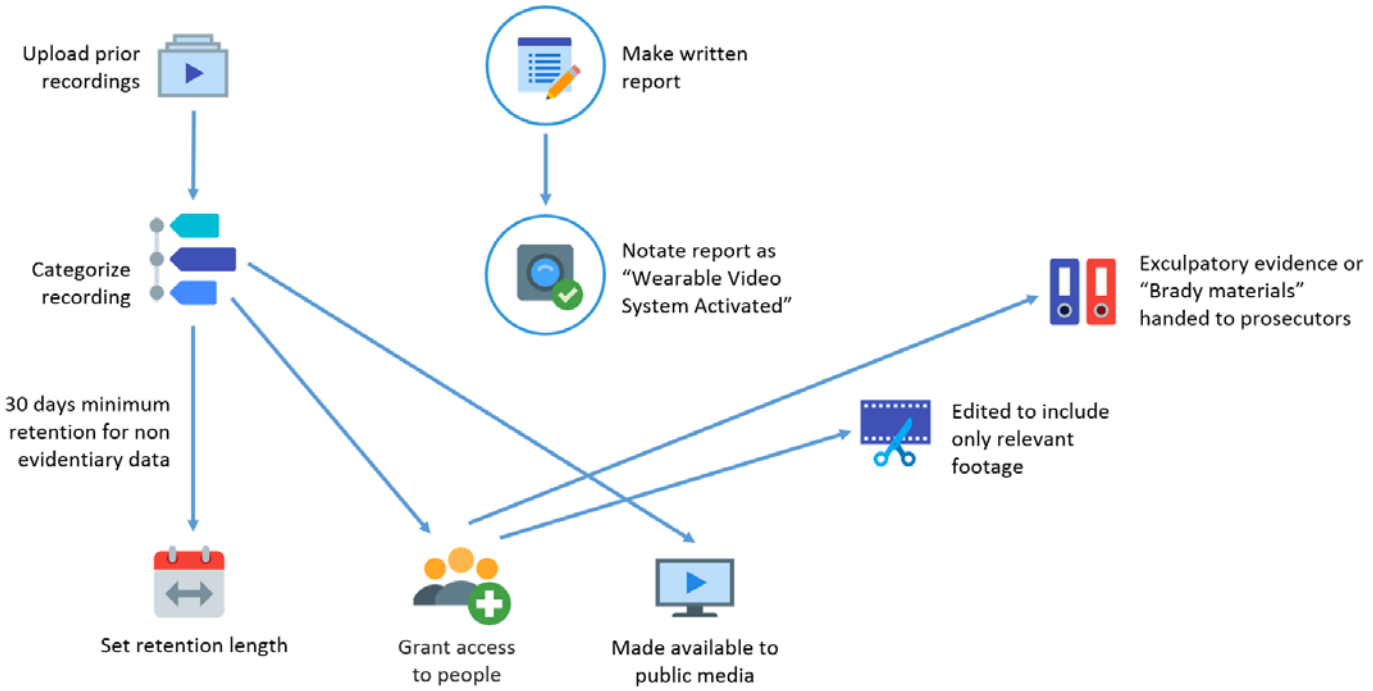
Therefore, various methods must be considered. This may include using a hybrid solution that initially uploads data to a cloud storage system for convenience, and then extracts the data from the cloud and stores evidence in on-premises storage for analysis and retention. Although agencies may tend to focus on the cameras themselves, it is important to realize that storage costs are the most important expense in the long term.

The Bigger Truth

The challenge for body camera storage is to understand the implications of this type of evidence. With the rapid adoption of digital body cameras, it is tempting to take the expedient approach to use the default storage system offered by camera suppliers.

However, it is important to create a long-term plan for storing the video evidence generated by these devices. Law enforcement agencies need to step back and understand that video evidence storage has complex long-term requirements that are a combination of traditional IT storage needs and law enforcement evidentiary requirements. Default cloud-based storage may be easy to deploy but it places one on a single narrow path, while a more holistic approach that incorporates on-premises storage, perhaps augmented by cloud-storage, will take multiple considerations into account (see Figure 4).

Figure 4. Example Evidence Collection Workflow



Source: Enterprise Strategy Group, 2016

For example, consider a crime scene that needs multiple agencies involved and is part of a long-term investigation. In that case, evidence for the case may include arrest or pursuit videos on body cameras, dash camera videos prior to the arrest, photographs taken at the crime scene, and the requirement to share the evidence with other agencies such as at the state or national level. If the case affects national security, then the requirement for retaining the evidence may span many years, exceeding those required for local cases.

The top considerations that organizations must grapple with when deciding on a method for storing video data from body cameras are the total cost of ownership, the value of an integrated storage platform, management/collaboration, and regulatory compliance. Finding a system that incorporates all of these requirements is the best way for an organization to meet its departmental goals, balancing cost and the very real needs related to providing service as a criminal justice agency. This is an issue that has an impact on law enforcement agencies, metropolitan IT departments, and taxpayers alike.

The challenges and associated considerations include:

- Cost: Examine the total cost of storage, and apply the appropriate methods for each type of evidence.
- Integration: Coordinating with workflow for different types of evidence.
- Management: Following SOPs for evidence, protecting its integrity and organizing it in accordance with existing record management processes.
- Compliance: Meeting legal requirements such as CJIS or data storage location as required by law.

It is tempting to choose a cloud-based storage system from the camera vendors themselves, since they are offered alongside the acquisition of the body cameras. However, it is critical to approach the purchase with a balanced and holistic

view that reviews the long-term (five-year) costs for equipment and public cloud storage, and compare that to the deployment of an organization's own storage infrastructure, or the implementation of a storage methodology from a service provider that serves law-enforcement-specific needs. Long-term commitments to cloud storage are often made in early phases of a body camera pilot and before a full scale body camera deployment is fully realized. That is dangerous since it ties the budget to a particular implementation before the results are properly evaluated.

Law enforcement video storage is unlike the comparatively simple world of consumer-class cloud storage, such as that which provides capacity for music or other personal media. Video evidence comes with requirements for handling that may span decades, and body cameras represent a relatively new technology where public cloud evidence storage is still relatively untested. It is important to keep video evidence storage infrastructure under an organization's own control so that the system can evolve and be integrated with rest of the law enforcement infrastructure.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188