Panasonic

DATA STORAGE: AVOID THESE COSTLY MISTAKES

As agencies across the country grapple with changing video storage and retention law and policy, flexibility is key to any evidence management system

By Panasonic Arbitrator Body-worn Camera Product Manager and former Police Officer John Cusick.

Looking at some of the largest police departments in the country, it's possible to draw a few conclusions about data storage: First, there is no "one size fits all." Because departments vary in size and regulations, data storage needs and requirements differ by state, region and municipality. Second, many law enforcement organizations continue to re-evaluate their data storage needs and policies as technology, laws and their regulations continue to change.

Technology is changing policing, and that's nothing new. In the early 20th century, police grappled successfully with what was then a new technology called fingerprinting. Later, in the 1960s, came the first 911 emergency call service, which ushered in a new way of working for many officers. Today, determining how to manage data evidence is among the biggest challenges facing agencies large and small. Some law enforcement organizations are hiring workers dedicated to handling FOIA requests, managing videos that must be stored for long periods and redacting videos to protect privacy. Others are enlisting the help of private industry.

Panasonic works with agencies across the country, and what we've heard consistently are differences in how police are dealing with evidence management and ways in which they're struggling with new technologies. Based on our conversations, we see three areas where mistakes most often happen when it comes to evidence management. Here's a look at the most common mistakes and ways to avoid them.

Mistake 1: Failure to calculate how much data storage they'll need

According to a study by the Major Cities Chiefs and Major County Sheriff's Association, 42.03% of its respondents – made up of law enforcement officials – didn't know how much data their officers would be generating on a daily basis. Here is a good place to start: Begin with the number of body-worn cameras used daily. Multiply that number by the average number of hours the cameras is used every day, and by the retention time—on average. Then factor in other evidence the agency might have to store, such as footage from still cameras, documents, video from fixed cameras, or any other data you may want to store within your evidence management system. Keep in mind also that changes in retention policy can also impact storage calculations.

Our solution: Use a flexible data management system

An evidence data management system will work as an interface between the user, their applications and their data to organize and analyze content that has been captured. If the evidentiary data is being held on-site, it can be managed through software but, as cloud computing becomes more prevalent, web applications are being developed to manage content both on-site and in the cloud.

Here's a typical scenario: a law enforcement agency has been using dashboard cameras for the last five years and has exhausted its on premise data storage. Meanwhile, it has added hundreds of body-worn cameras, and faces new requirements dictating when a camera should be activated—from issuing a summons to conducting a car stop, to making an arrest. The end result: more data than available storage.

In this scenario, the agency decides to move its newest video from its body-worn cameras to the cloud. That's because the cloud brings new capabilities when it comes to recovery, retention, and redundancy. When dealing with data that has an important role as evidence, consideration of all these issues is paramount.

In a cloud implementation, all these features are built into the technology's platform. In teaming with CJIS-compliant Microsoft Azure Government, Panasonic is offering multi-tiers of storage platforms managed by its UEMS – "Unified Evidence Management System" server to move content from either on-premise to cloud or even, to long-term archival solutions using Blu-ray and optical discs.

A growing number of agencies are turning to the cloud for data storage or—a third possibility—a hybrid storage solution that allows some data to be stored on premise, and some in the cloud. We see agencies considering a custom hybrid option when they realize how quickly their on-site storage resources will need to increase.

Mistake 2: Failure to establish the right procedures prior to BWC implementation

On the granular level, data retention for BWC footage can become complex. Retention policies must meet federal, state, city and local guidelines that give agencies guidance on how long they must retain the evidentiary data and when it can or cannot be disseminated. There are different guidelines for different scenarios. The recording for a major event, for instance, may need to be retained for a longer period of time than a simple report call.

Our suggestion: identify and collaborate with the right appropriate stakeholders early

In an analysis of retention and release policies across the country, the Brennan Center for Justice at NYU wrote that one of the biggest questions surrounding BWCs is whether the video will be eligible for public release under public records laws. And the answer to that question is still up in the air, in many states, as legislatures debate bills to address the issue.

The good news is that a sophisticated data management system can be configured to monitor and maintain these processes to ensure adherence to these policies. Still, when it comes to developing the specific protocol, it can be helpful to collaborate with local and city officials. This way, the different governmental offices are all working together with law enforcement to clearly define actionable procedures that follow policy.

Once this protocol is set in place, the data management systems can then be configured to automate many aspects of the defined retention and management policies regarding the storage and access to the evidentiary data.

Mistake 3: Choosing an unreliable vendor

The BWC market is a new one for many companies and, with so many law enforcement agencies planning to implement BWC programs over the next few years, vendors see this new market as an opportunity for growth. This means more choices and opportunities to find the right solutions for agency needs, but it also allows for inexperienced vendors to enter the market. Do providers under consideration have a history of reliability, the infrastructure to handle all of your needs, and experience working with law enforcement? These are important questions to answer before making a decision.

Our suggestion: do your homework

Picking the right company to partner with is one of the most important decisions a any law enforcement agency can make when implementing a BWC program along with a robust data management system. Some agencies are under tremendous pressure to act quickly and with a lean budget.

Before deciding, try a pilot program and ask about the provider's longevity. Is it poised to maintain a steady business and remain a reliable partner for years to come? One indicator is the way in which the solutions provider addresses changing technology and customer feedback. Are they willing and able to pivot with new capabilities as circumstances warrant?

Companies with the right resources and a history of collaborating with law enforcement can operate as a true partner, customizing each solution to fit the specific needs of each agency. Considering how granular those needs can become when developing procedures based on local, city, state and federal regulations, the ability to adapt and provide a complete solution with full support is paramount and will serve your agency well in the long run.