Carl Brooks, Consultant
PRI Management Group

Constantly changing technology. A profession always seeking ways to adapt to the changes. That is law enforcement in 2023.

In recent years, a particularly challenging issue has been the proliferation of digital evidence management systems (DEMS) and the myriad companies who promise a complete solution. With the rise in the use of body-worn cameras (BWC), in car cameras, and the almost ubiquitous use of video footage in every case from trespassing to homicide, the need for a practical, efficient, and affordable response has become a pressing concern. This, coupled with the call for budgets cuts and ever diminishing resources, has administrators struggling to adapt while trying to establish a viable digital evidence process for their agencies.

For decades, the profession considered the only type of "digital evidence" was keeping an electronic copy of a police report. Now, however, it's a host of other items as well. On any given day, agencies across the nation store volumes of computer files, VOIP and analog phone data, RMS use logs, victim and witness statements, lab reports, DNA results, CAD calls, in-car camera footage, BWC footage, and private security footage to name just a few. In command staff meetings across the nation, administrators jostle ideas about trying to find ways to address this proliferation of digital media while also trying to deal with the ever-rising cost of storing that media.

However, most agencies do not have a robust storage and retrieval mechanism for this digital evidence, or a plan in place to deal with the ever-growing amount of digital evidence they possess. Without systems in place, the data is useless, costly to maintain, and can pose challenges for the agency in court, and in the court of public opinion.

An "old school," but practically standard way to address this issue is the use of CD/DVD's and, in some places, even VHS tapes. These, however, are antiquated means of keeping digital evidence, and are costly, can be labor intensive, and are often unreliable. Many agencies still manually transfer files between CD/DVD's then "snail" mail them or physically transport them to evidence storage or court.

Over time, the files on the CD/DVD deteriorate, the CD/DVD's themselves are hard to catalog, and the data on them is difficult to search through. Even the method used to label the discs for later retrieval – pens and markers - damages the quality of the evidence on the disc.

CHAIN OF CUSTODY AND STORAGE

The chain of custody is also difficult to maintain. While agencies can track the physical disc, there is no real way to track the viewing of the media contained on the disc or logging who may have downloaded copies. When using this storage method you also don't really have a way of proving if the media contained on the disc was altered prior to the "burning" of the disc or if altered versions of the media exists on other copies.

Storage sizes of the discs are often limited and there may be dozens, if not hundreds, of discs for a single large case. This leads to storage issues, retrieval issues, and prohibitive costs for the continual resupply of the discs.

How video is captured and stored also presents significant issues. BWC video is often stored on a proprietary website that is separate from the in-car footage, which in turn is stored separately from investigator's voice interviews and other "regular" evidence.

Various media types are stored in multiple different formats which requires several systems simply to play back the files. This makes the job of investigators very challenging as they try to piece all the various digital evidence together from these disparate locales. This also causes challenges for the prosecution when evidence is spread among so many formats and in so many places.

The best solution is for agencies to develop a dynamic and comprehensive digital evidence management process with cloud capability. However, where does one begin to develop that for an agency? Consider the following:

→ Does the average agency member know if the vendor charges per upload and download?

→ Do they charge based on storage amount and if so, how much?

→ For the users, is there a yearly fee per license?

→ Do you still own your data after you upload or does it become proprietary?

→ Once you upload, will the media still be compatible with your viewers and the viewing capability of the courts?

→ Can the media be shared easily among other agencies and the prosecutor's office?

→ Once the media is uploaded can the agency retrieve it easily?

→ Can the media be redacted and are there options for automatic and bulk redaction?

→ Are there audit logs and the ability to remove PII (personally identifiable information)?

All of these are important questions to ask but they aren't the only information needed.

RETENTION

Keeping everything forever is a risk, including records *and* evidence. Consider the following:

- → Does your agency have a solid and consistent annual records and evidence purge process in place?

- → Are records and evidence kept beyond retention periods?

- → Does the agency have policy governing the process and timeframes for destruction of these entities?

- → Does the agency utilize spreadsheets or logs for tracking retention, disposition, and purging of evidence and records?

- → Does the records unit and the property/evidence unit work together closely to reconcile evidence and the related case files so purging is done together?

- → Are retention schedules updated and current with law and best practice?

These questions are all vital in the selection of the right system and, equally important, the development of an agency records and evidence management program that is governed by policy.

Soon, the amount of digital evidence will exceed the amount of "regular" evidence in the possession of most agencies.

As an agency are you ready when that day comes?

HOW PRI CAN HELP

PRI can help identify areas of risk, build policy, and re-engineer processes to achieve compliance and maximum productivity. We develop retention schedules, system requirements, and the specifications necessary to select the right digital evidence management system for your needs to align with agency workflows, policy, and procedure.

Since 2008, PRI has been exclusively helping law enforcement agencies procure, manage, and implement systems, records, digital evidence, and data in the most cost-effective and efficient manner while ensuring their compliance with the maze of governing public records, NIBRS, and technology standards.

Contact us for assistance with your records and technology needs at info@policerecordsmanagement.com. See policerecordsmanagement,com for further information.