The Next 5 Years Are Crucial:

WHY DIGITAL EVIDENCE IS BOTH YOUR BIGGEST CHALLENGE AND YOUR BIGGEST OPPORTUNITY

DIGITAL EVIDENCE IS INCREASING EXPONENTIALLY

The Boston Marathon bombing in 2013 was a turning point in the digital evidence landscape. It was one of the first major incidents in the U.S. that happened in the age of smartphones in every pocket and surveillance systems at every storefront. Tens of thousands of images and hours of video footage flooded in from bystanders and surveillance cameras. Thanks to this footage, forensic analysts were able to identify and release an image of the suspects within just three days.

Large incidents like the Boston Marathon bombing or the January 6th attack on the U.S. Capitol can generate hundreds of thousands of crowdsourced video and photo submissions, and collecting, storing, and processing these images requires technology that many law enforcement agencies aren't keeping pace with.

omnigo

It's not only large incidents that generate a lot of digital evidence, though. Many typical law enforcement incidents now generate over 1TB of evidence, and the amount is exponentially increasing.

It's no longer only computer files, phone records, and business security systems generating digital evidence, either. Crime-scene images, fingerprints, DNA analysis, lab reports, victim and witness interviews, expert testimonies, 911 calls, and emergency responder radio traffic data – all of it is stored digitally. Plus, there's mounting evidence coming from communications and cloud service providers, sensors, biometrics, videos from bystanders, and surveillance systems at private homes and businesses.

In addition to electronic reports, investigative digital evidence, and community-generated digital evidence, officers generate hours of video from in-car and body-worn cameras. In fact, more and more states are passing legislation to mandate body worn cameras and storage requirements for the footage. According to the National Conference of State Legislatures, legislatures in seven states passed such mandates between 2020 and 2021 (Colorado, Connecticut, Illinois, Maryland, New Jersey, New Mexico, and South Carolina), and the list is growing.

Our ability to generate digital evidence is exploding, and policing is becoming a high-tech profession. Yet, most departments aren't keeping up with the demand to efficiently collect, store, organize, synthesize, analyze, and utilize it all.

POLICING IS BECOMING DIGITAL: IS YOUR AGENCY KEEPING UP?

Do you have the space, time, resources, and knowledge required to manage over 1TB of digital data for each case? How long would it take you to find, organize, synthesize, analyze, and utilize all of the digital data associated with a single case? What falls through the cracks when you can't manage it all?

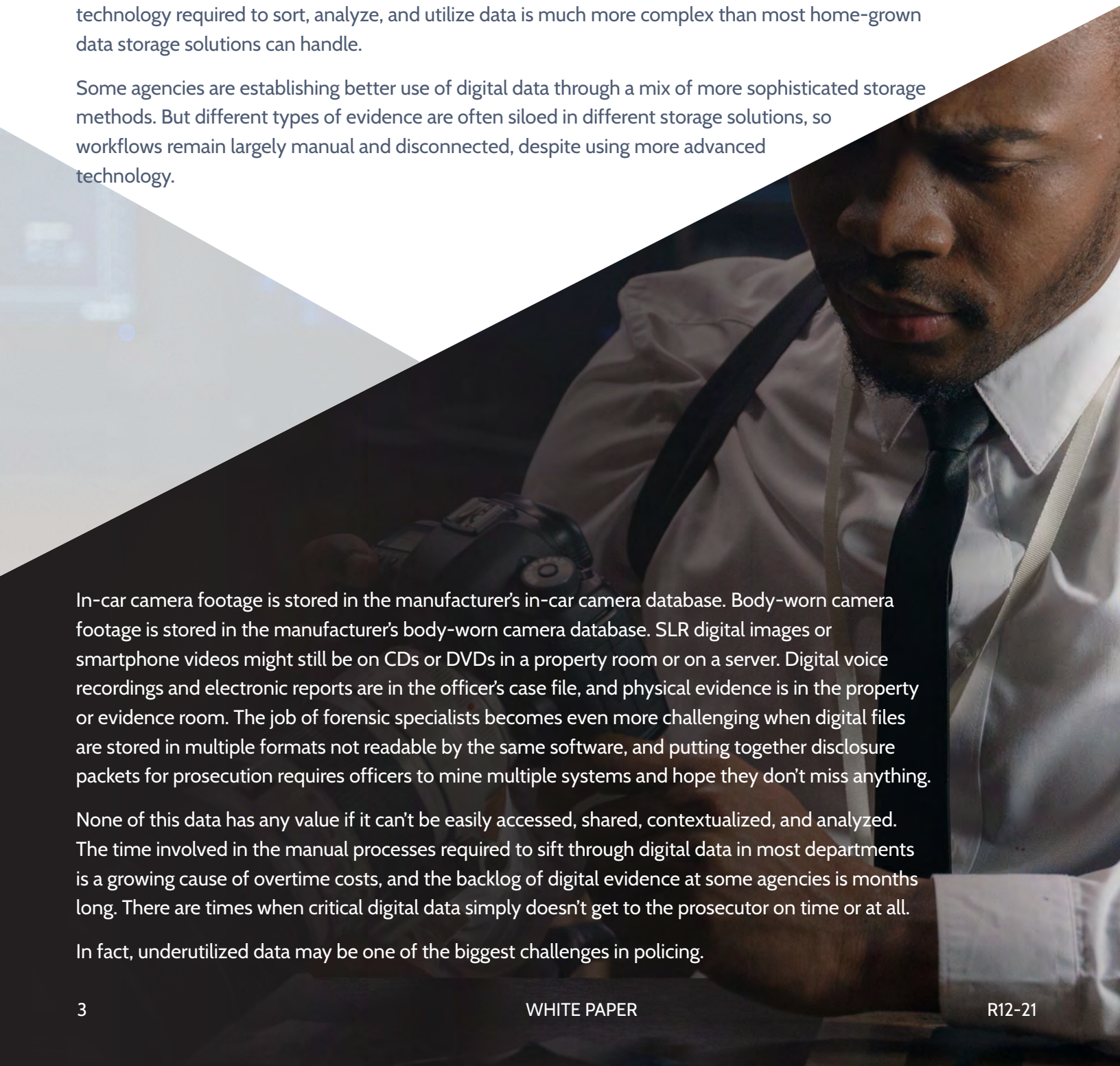
In theory, more data should lead to better outcomes. But if you don't have an easy, intelligent system in place to organize, protect, analyze, and contextualize your data, you can't use it – and in the worst-case scenario, your perpetrator will go free when the evidence to convict him was right under your nose.

Many agencies are still storing evidence and data on CDs, DVDs, or on-premises servers. These antiquated solutions are labor intensive, prone to error, and often forensically unsound.

As digital evidence becomes easier to manipulate, it's even more important that prosecutors can ensure proper chain of custody. How can you prove that nobody has tampered with your digital evidence and the data you provide is authentic and unchanged? Can you prove that the evidence was logged accurately and that access to it was properly controlled? Can you easily utilize your digital evidence to develop an accurate timeline and tell a straightforward story of the case? When you can't, it creates reasonable doubt in the minds of jury members.

Antiquated systems for managing digital evidence cost agencies time and money and cost communities justice. CDs and DVDs are manually copied, physically mailed, or personally transported in each step of the process. Discs deteriorate and get misplaced. Storing digital files on servers also poses problems. It's difficult to find data by case number, uploader, or even date. The technology required to sort, analyze, and utilize data is much more complex than most home-grown data storage solutions can handle.

Some agencies are establishing better use of digital data through a mix of more sophisticated storage methods. But different types of evidence are often siloed in different storage solutions, so workflows remain largely manual and disconnected, despite using more advanced technology.



In-car camera footage is stored in the manufacturer's in-car camera database. Body-worn camera footage is stored in the manufacturer's body-worn camera database. SLR digital images or smartphone videos might still be on CDs or DVDs in a property room or on a server. Digital voice recordings and electronic reports are in the officer's case file, and physical evidence is in the property or evidence room. The job of forensic specialists becomes even more challenging when digital files are stored in multiple formats not readable by the same software, and putting together disclosure packets for prosecution requires officers to mine multiple systems and hope they don't miss anything.

None of this data has any value if it can't be easily accessed, shared, contextualized, and analyzed. The time involved in the manual processes required to sift through digital data in most departments is a growing cause of overtime costs, and the backlog of digital evidence at some agencies is months long. There are times when critical digital data simply doesn't get to the prosecutor on time or at all.

In fact, underutilized data may be one of the biggest challenges in policing.

UNDERUTILIZED DIGITAL DATA MAY BE ONE OF THE BIGGEST CHALLENGES IN POLICING

What are the consequences of underutilized digital data?

Missed Critical Connections and Patterns

When digital data is siloed in disparate storage systems, it's not easily contextualized, and it becomes difficult to draw the right connections.

Perceived or Actual Bias

When resources are limited, some departments have to be selective about which cases will receive a complete analysis of the digital evidence.

Reduced Awareness

When it's difficult to share relevant digital evidence with neighboring jurisdictions, critical awareness is lost.

Lost Time, Lost Convictions

When there are months of backlogs and more data than a department can handle, prosecutors don't get digital evidence on time to prepare properly, and sometimes they don't get it at all. According to a publication by the RAND Corporation, more cases are being solved on digital evidence than anything else. Communities can't afford to skip this step.

THE EFFECTIVE SOLUTION THAT TURNS DIGITAL EVIDENCE INTO POWERFUL PROOF

The best solution to the digital data deluge is a robust, cloud-based digital evidence management system (DEMS). A purpose-built DEMS provides more than merely storage. It provides automation, intelligence, security, and transparency. It also provides a single end-to-end solution that meets the needs of the entire justice system, from the officers responding to 911 calls to the prosecutors who need to prepare and share a complete evidence package. An integrated, scalable, searchable solution will bring unprecedented efficiency, insight, accuracy, and security to your investigations and will free up valuable officer time to enable increased community presence.

WHAT FEATURES AND BENEFITS WILL A GOOD DEMS OFFER?

Integration

Look for a DEMS that will integrate with all of your systems that generate digital data, such as in-car and body-worn camera systems and computer aided dispatch (CAD) and records management systems (RMS). When data can be rapidly or even automatically submitted to your DEMS, it reduces the risk of loss or compromise.

Unification

A DEMS will unify all of your digital data in one simple place. View videos in disparate formats side-by-side for comparison and insight. Visualize patterns, connections, and timelines that would be difficult to establish without easy data unification.

Accessibility

Officers can make evidence immediately available across the criminal justice system in minutes, without ever leaving the street. Anyone with the proper permissions can access or securely share evidence from any computer, any time of the day or night.

Security & Defensibility

Security features enable customized permissions and record who accessed (or tried and failed to access) what and at what time, ensuring complete chain of custody for all digital evidence.

Authentication

Authenticate digital data to prove it's original and untampered with.

Searchability

Metadata associated with each piece of evidence in a DEMS makes it easy to find what you need quickly.

Compliance

A DEMS can ensure you're complying with local, state, and federal regulations and that you're following security standards set by Criminal Justice Information Services (CJIS).

There are a number of features to consider when investing in a DEMS, including flexibility, scalability, and expertise. Not every department needs – or can afford – every feature offered in a system. Look for software that is flexible and scalable to meet your needs now and in the future. It's also important that the manufacturer you choose doesn't only have expertise in software, but also has expertise in law enforcement. Software developed by law enforcement professionals, for law enforcement professionals, will be purpose-built to meet your unique challenges.

A DEMS SOLVES MORE THAN THE DIGITAL EVIDENCE CHALLENGE

Effective digital evidence management leads to actionable insights that keep our communities safer, and it also provides opportunities to solve other operational and societal challenges.

Increase Community Presence

When officers spend less time manually managing digital evidence, they can spend more time in their communities. This is especially important right now, when departments are struggling with officer hiring and retention at the same time they're being asked to spend more time on community outreach and relationship building.

Justify Spending

Using digital evidence management software results in less administrative overtime and more officer time in the community, making it easy to demonstrate ROI, which is increasingly important as police budgets are tightening.

Increase Accountability

Calls for increased police accountability are growing. Having a well-managed, easily accessible archive of officer-generated footage from body-worn cameras and other data related to officer response makes it easy to implement accountability protocols.

Demonstrate Effectiveness

Demonstrate effective policing to your community by harnessing the evidence-based insights your digital evidence software helps you generate.

Gain Public Trust

According to a survey by the Police Executive Research Forum, the most important priority for police in 2021 (chosen by more than three-fourths of respondents) is increasing public trust in police. Having a secure, reliable process for storing, accessing, analyzing, and auditing digital evidence lends itself to the transparency in policing that communities demand.

Enable Agility

The digital evidence landscape will continue to evolve at rapid speeds. Switching to an automated, cloud-based system for managing digital evidence will allow you to pivot more easily when priorities, protocols, and technologies change, without the operational impediments outdated systems can impose.

WHAT ARE THE IMPEDIMENTS TO IMPLEMENTING A SOPHISTICATED DEMS?

There are a number of challenges that prevent police department from implementing ideal DEMS.

Budgets are tightening across law-enforcement agencies. Some departments don't know how to justify a large technology expenditure when they need more officers in the field.

Most departments recognize that they are overwhelmed with the enormous quantity of digital evidence associated with each case, yet cognitive and cultural bias toward the old way of doing things remains strong. Some officers or departments aren't comfortable embracing a drastic change in the way they work.

HOW CAN DEPARTMENTS OVERCOME THESE IMPEDIMENTS?

Streamlining and automating administrative activities related to managing digital evidence reduces overtime costs and frees up hours for officers to spend in the field. Digital evidence management software is force multiplier that contributes to the best outcomes for the community and can ultimately save costs. And, with the increasing mandates for body-worn cameras, states are also increasing funding for technology purchases to support those mandates.

Like the private sector, police must embrace a culture of innovation. New technology and new ways of doing things are often met with resistance. But familiarity and education help propel departments into the future. For instance, just five years ago, there was still a lot of skepticism about body-worn cameras. Now police chiefs want them, and states are mandating them. Changing a culture can be done with persistence, leadership, and education. Community concerns about bias in AI, privacy, and surveillance can also be quelled with familiarity and education. Develop clear protocols for how your department uses technology in policing, and enforce them. Ensure that citizens in your jurisdiction understand the technology you use, how you use it, and how it keeps their communities safer.

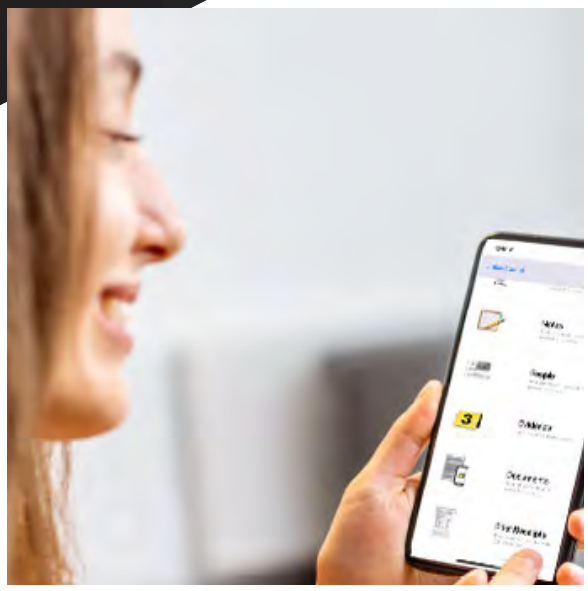
ARE YOU READY TO EMBRACE INNOVATION THAT KEEPS YOUR COMMUNITY SAFER?

The digital evidence deluge will only get worse over the next five years, but it doesn't have to be detrimental. Turn this challenge into an opportunity by investing in a digital evidence management system that addresses more than just the digital evidence challenge. It's the modern solution to many modern policing problems.

ABOUT OMNIGO

For more than 20 years, Omnigo software solutions have been the preferred choice for law enforcement, education, healthcare, gaming, hospitality, and corporate enterprises. Currently, Omnigo's solutions are used by over 2,000 customers in 20 different countries. At Omnigo, we're committed to helping customers secure their organizations' property, control operational costs, and ensure the safety of the general public.

We believe our customers deserve the best support available to protect their people, assets, and brand. We also understand how challenging it can be to protect the community without the proper resources. We're here to arm users with the best tools in the industry. With a team that includes former law enforcement, first responders, and other public safety professionals, we're uniquely qualified to understand exactly what our customers need to protect their community.



LEARN MORE OR REQUEST A LIVE DEMO

call: 866.421.2374
email: sales@omnigo.com

omnigo