Microsoft

The Insider's Guide to Police Body-Worn Video

New For 2016

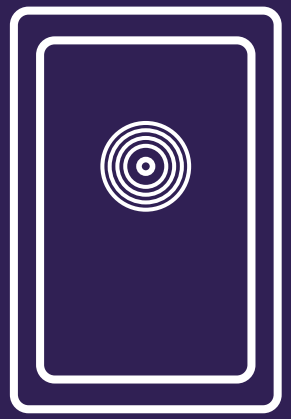
Now with the three-fold process for handling criminal justice information

TABLE OF CONTENTS

Introduction

"Since Ferguson, the adoption of cameras has only accelerated. It is easy to understand why: greater accountability for police; better evidence of crimes; an unbiased record of facts. But before we adopt this technology everywhere, we need a realistic grasp on the sheer volume of data involved."

Body-worn cameras reduced the use of force by roughly 60 percent in Oakland, California, and the department reported 18 months without an officer-involved shooting, in a city that used to average about eight such incidents a year. The San Diego Police Department saw similar results: after their 14-month study, their use of force incidents decreased by 47%. In Mesa, Arizona, police reported 75 percent fewer use of force complaints and a 50 percent decline in citizen complaints during a body-worn camera pilot. As agencies around the world are starting to recognize, the benefits of body-worn cameras go beyond use of force and aid in evidence gathering and improving practices through training. A "hugely successful" trial of the technology in New South Wales, Australia resulted in a $4 million investment in body-worn cameras throughout the state.



Body-worn cameras reduced the use of force by roughly 60 percent...

[1]Michael Chertoff, 2014. "Local police learn to bear body cameras". USA Today.
http://www.usatoday.com/story/opinion/2014/10/22/police-body-cameras-privacy-cloud-column/17744917/

[2]2015. "Increased Protection For Police And Public With Rollout Of Body-worn Video Cameras". The Indian Telegraph.
http://theindiantelegraph.com.au/increased-protection-for-police-and-public-with-rollout-of-body-worn-video-cameras/

Early users cite numerous practical applications and benefits from having law enforcement officers wear cameras, including:

- **Documenting evidence.** Cameras provide evidentiary benefits, including expedited resolution of citizen complaints and lawsuits.

- **Officer training.** With capture of in-the-moment officer behavior, video presents excellent training and coaching opportunities for how best to handle an incident.

- **Preventing and resolving complaints brought by members of the public.** Improvements have been shown in both police and citizen behavior when cameras are worn in a visible location.

- **Strengthening police accountability.** Cameras provide transparency, which can improve police accountability and performance.

- **Secure cloud storage.** To support retention, analysis and collaboration, video can be securely stored in the cloud through a provider with a contractual commitment to a compliance organization such as the such as the FBI's Criminal Justice Information Service (CJIS) Security Policy, the UK Government G-Cloud, the Singapore MTCS SS Tier 3 certification, or the Australian Signals Directorate CCSL IRAP standard.

Today, law enforcement agencies across the globe are dealing with body-worn video footage as a new form of criminal justice information that needs to be collected, stored and managed with security in mind. Once collected, these petabytes of new footage become a part of law enforcement's greater video ecosystem, and thus should be perceived as such and protected accordingly.

The International Association of Chiefs of Police (IACP) recommends that all criminal justice information collected in jurisdictions within the United States, including body-worn video footage, be safely and securely stored, analyzed and managed. IACP recognizes the importance of cloud services in dealing with the high volume of information collected through the use of this new technology and, as a result, has developed a set of Guiding Principles on Cloud Computing for law enforcement to consider. These principles point law enforcement toward the importance of compliance with the FBI Criminal Justice Information Services (CJIS) Policy, which serves as a baseline set of regulations to manage criminal justice information in today's complex and digitized environment.

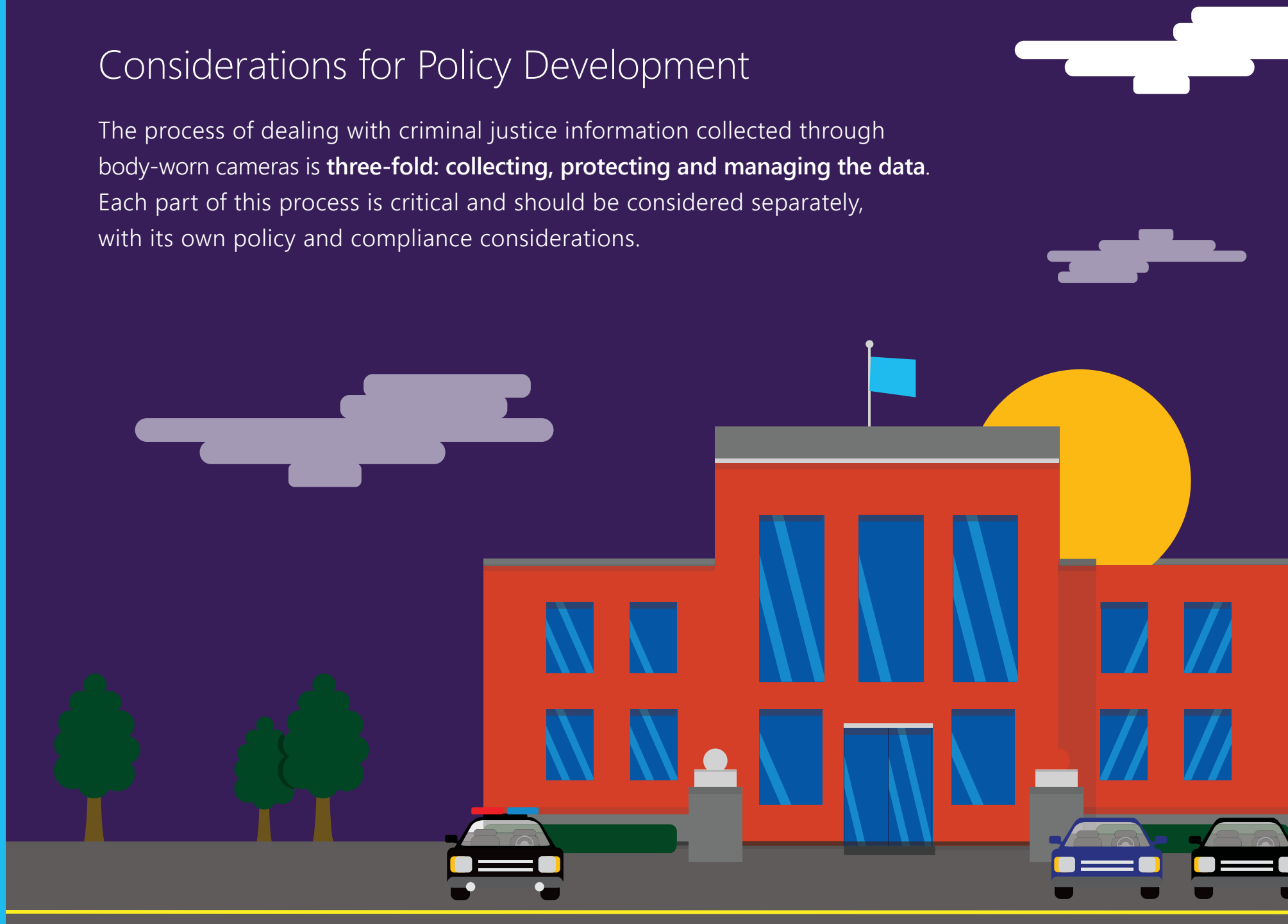
The CJIS Policy offers a strategy to help law enforcement safely and securely store, analyze and manage that information. IACP recommends that law enforcement choose a cloud solution that supports CJIS compliance for the complete lifecycle of criminal justice information—regardless of how long that information must be stored and how it's assessed and managed.

Similarly, international jurisdictions in the United Kingdom, Australia, Europe, Singapore and elsewhere can rely on security standards. These standards have been established to help law enforcement ensure that criminal justice information is stored and managed with the utmost attention to security in the cloud.

These standards have been established to help law enforcement ensure that criminal justice information is stored and managed with the utmost attention to security in the cloud.

Considerations for Policy Development

The process of dealing with criminal justice information collected through body-worn cameras is **three-fold: collecting, protecting and managing the data**. Each part of this process is critical and should be considered separately, with its own policy and compliance considerations.



Part 1 :

Collecting the Information

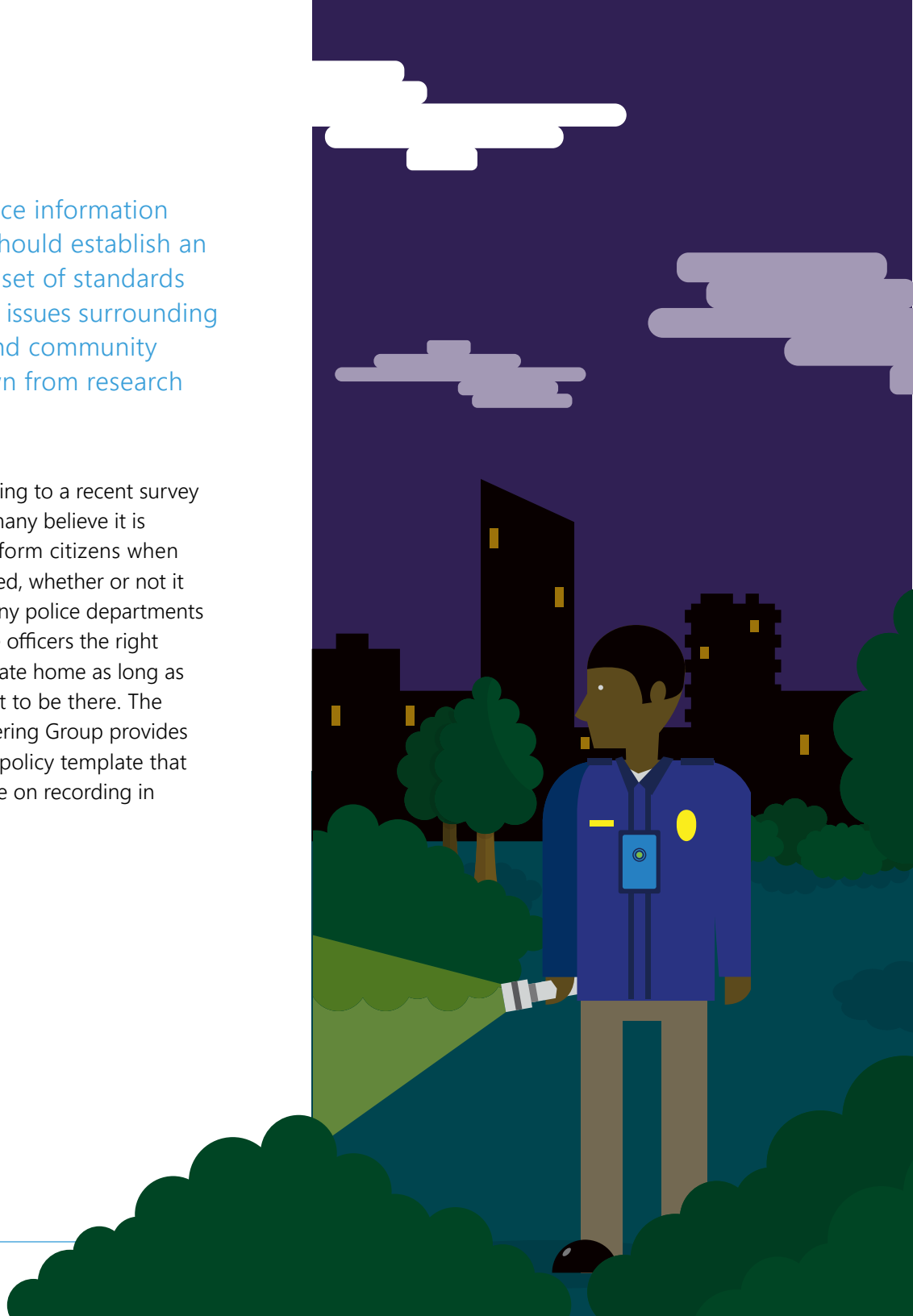
Collecting the Information

Controversy surrounds the issue of collecting criminal justice information through body-worn cameras. Law enforcement agencies should establish an in-house policy that effectively unifies the agency under a set of standards to avoid liability and confusion. This policy should address all issues surrounding collection—including recording practices, privacy issues and community relationships. The following policy considerations are drawn from research and examples of other agencies that have led the way.

- **When to record** – Early adopters offer differing opinions on whether to allow officer discretion for turning cameras off. Some departments leave them on all the time and others require turning them on at the beginning of an incident. Many agencies report allowing for limited discretion by officers, provided there are clear requirements to document reasons for not recording.

  A common approach is to require officers to activate cameras when responding to calls or during any enforcement activity with the public. "We try to develop muscle memory in officers to turn on cameras enroute to a call," one police chief advised, "because it's easy for them to forget once they're engaged." Typical exceptions include interviews with sexual assault victims or hospital visits, or conversations with confidential informants.

- **Notification** – According to a recent survey of police executives, many believe it is a good practice to inform citizens when they are being recorded, whether or not it is required by law. Many police departments have policies that give officers the right to record inside a private home as long as they have a legal right to be there. The Body-worn Video Steering Group provides a body-worn camera policy template that gives specific guidance on recording in private dwellings.



- **Citizen privacy** – Body-worn cameras capture crime victims in traumatic experiences, often in their own homes, as well as witnesses and confidential informants. Privacy considerations need to be balanced against the need for police transparency and evidence collection. Some agencies are choosing a flexible, discretion-based approach, while others require more stringent procedures. One agency now requires consent to be obtained from crime victims before officers record an interview. "This new policy is a response to the privacy concerns that arise when you are dealing with victims of crime," said one police chief regarding these measures.

- **Community relationships** – Police rely on positive community relationships to do their jobs. Policies need to include open communications about cameras with community members in order to respect and protect these relationships. Some agencies have faced challenges with body-worn cameras when working with partners in the community, while others have not noticed any difference in community relationships. One agency reported using footage to address concerns of racial profiling during traffic stops that were raised by a community organization. The agency used the new technology to identify and correct the problem while strengthening the relationship with the community.

Policies need to include open communications about cameras with community members in order to respect and protect these relationships.

Part 2 :

Protecting the Information

Protecting the Information

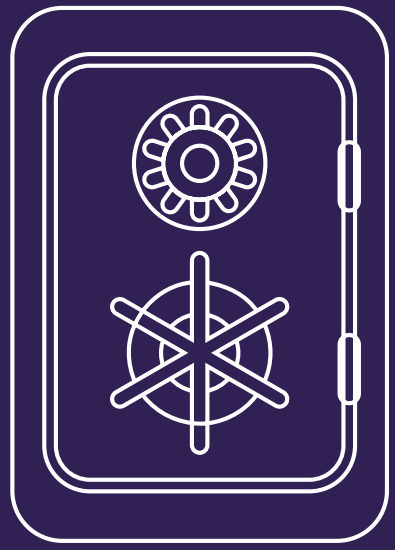
Body-worn video, along with fingerprints and other valuable digital criminal justice information needs to be provided the greatest degree of protection possible. And yet IT staff in jurisdictions around the world are facing strained resources as a result of increased video-related workloads. It used to be that video recordings were retained for 30 days, per municipal standards. In today's volatile environment, however, the new normal dictates keeping video recordings for a minimum of 90 days, and sometimes permanently.

With retention periods increasing so dramatically, the video workload is surpassing departments' management and budgetary constraints, increasing the need for secure cloud computing solutions. Leveraging the cloud for video storage allows departments to focus resources back on law enforcement's primary mission: protecting the community.

Moving to the cloud brings to light the question of compliance. Without compliance, departments are at risk of new liability issues and audit concerns when deploying body-worn camera technology.

So how can a department move these large files to the cloud and remain compliant with national and international information security standards? Standards like the FBI CJIS Policy in the United States, InfoSec Registered Assessors Program standard in Australia, Multi-Tier Cloud Security in Singapore, the European Union's Safe Harbor standard and G-Cloud in the United Kingdom—create a safe and trusted working environment for agencies moving to the cloud.

In the United States, the CJIS Security Policy specifically covers data from the FBI. But It's a powerful standard for law enforcement to protect all of their data. The International Association of Chiefs of Police agrees—their updated cloud policy guides departments to hold all data to the CJIS Security Policy. The policy defines measures concerning security throughout the lifecycle of criminal justice information—from creation and collection to viewing, modification, transmission, dissemination, storage and destruction. Information system audits are required, whether completed automatically or manually. And the CJIS Policy defines other security measures, including access controls and secure login procedures.



In the United States, the CJIS Security Policy specifically covers data from the FBI. It's a useful baseline, endorsed by IACP, for law enforcement to protect all of their data.

Other countries around the world are helping pave the way for law enforcement's move to the cloud through initiatives that identify safe and trusted cloud providers and ensuring compliance measures are being met. Regardless of geography or jurisdiction, it's critical to find a cloud service that fully understands local compliance standards and is dedicated to providing compliance support. Before partnering with a cloud provider, there are a few questions agencies should consider:

- Does the provider support national standards, such as the FBI's CJIS Security Policy or the United Kingdom's G-Cloud, for protecting criminal justice information?

- Does the provider contractually commit to managing data in accordance with the national security policy?

- Does the provider have a separate, fully isolated cloud platform for U.S. federal, state and local government customers?

- Have the government personnel working in the cloud provider's data center passed a fingerprint-based background check adherent to the national or state security procedures?

With these questions in mind and a commitment to compliance, securing a cloud partner to entrust with large amounts of criminal justice information becomes more feasible for agencies of any scale.

Part 3 :

Managing the Information

Managing the Information

Governments around the world are endorsing the move to the cloud and ensuring that national security standards are being met. Once the information is moved to the cloud, how does that help law enforcement do better police work? Digital criminal justice information, including body-worn video, fingerprints and criminal records, needs to be accessed for cases, training and other law enforcement responsibilities. The following are a few ways in which cloud services can improve departmental efficiency:

Redaction – The cloud provides easy and seamless redaction for law enforcement, a high-level capacity that facilitates sharing videos and other digital information while upholding and protecting citizen privacy. Machine-learning Cloud-powered redaction reduces hours of manual redaction to minutes of effort on the part of officers preparing videos for dissemination.

Dissemination – Sharing videos with prosecutors and courts is essential to case work, and the current approach is to burn DVDs or save data to flash drives and physically share them. This method creates extra work for police and introduces levels of unnecessary risk, since these devices can get lost in the shuffle. Moving to cloud services means replacing this method with secure, remote viewing during which the video never has to leave the control of the police department.

Digital criminal justice information, including body-worn video, fingerprints and criminal records, needs to be accessed for cases, training and other law enforcement responsibilities.

Audio transcription and indexing – Audio transcription for videos aids in executing more powerful research, including keyword-based searches. One department revealed to Fortune magazine that police can search for specific keywords in the cloud database and retrieve the appropriate audio or video, making case work more efficient when it comes to body-worn video. Microsoft Azure Media Services has developed indexing for audio and video to help index spoken content within videos, allowing investigators to do exact in-video searches. This indexing service saves investigators hours of manual searching through video and audio clips.

On-demand resources – The cloud provides on-demand computing resources without up-front capital investment. This means that even small departments can leverage powerful tools that previously were only available to departments with their own sophisticated technology infrastructures. According to a recent IACP report, the "estimated savings by utilizing cloud services versus in-house equipment, labor, and infrastructure range from 30 to 50 percent."

[3]Vern Sallee, 2014. "Outsourcing the Evidence Room: Moving Digital Evidence to the Cloud". *The Police Chief 81. Page 42–46.*

Microsoft Azure: Designed for Law Enforcement Microsoft

Azure Media Services and Azure IoT can assist law enforcement in making digital police work more efficient. "Once we get our video onto the Azure platform," notes one officer who has deployed Azure Government cloud services, "we can aggregate it, we can learn from it, we can make the database proactive to tell us things." Microsoft Azure Media Services and Azure IoT can assist law enforcement in making digital police work more efficient. "Once we get our video onto the Azure platform," notes one officer who has deployed Azure Government cloud services, "we can aggregate it, we can learn from it, we can make the database proactive to tell us things." That's because Microsoft, which contractually commits to information compliance in the US and in other global jurisdictions, offers tools for law enforcement that make the most of cloud technologies to streamline investigative work or training within the department.

Law enforcement agencies around the world looking to adapt to present-day expectations of body worn cameras are in need of solutions to help collect, store, protect and manage digital criminal justice information. It is advisable to create a department-wide policy dictating collection procedures and then move storage, protection and management to the cloud. Through compliance-ready support and efficient features that save law enforcement officers hours of manual work, a cloud solution can solve the problems that accompany body worn video.

"Criminal justice information needs good security because it is information about citizens, often at their most distressed and vulnerable."

- Michael Chertoff,
  former secretary of the Department of Homeland Security

Microsoft Azure Government is the CJIS-capable cloud designed for law enforcement. Visit **http://aka.ms/cjis-cloud**.

[4]Jonathan Vanian, 2015. "How Microsoft is courting law enforcement to its cloud". Fortune. *http://fortune.com/2015/06/24/microsoft-police-cloud-data/*

Through compliance-ready support and efficient features that save law enforcement officers hours of manual work, a cloud solution can solve the problems that accompany body-worn video.

microsoft.com