



## MAJORITY REPORT: EVIDENCE IN A CONNECTED WORLD

A Bitcurrent analysis of TASER International's AXON/Evidence.com service  
and the state of video recording in law enforcement.

---





## INTRODUCTION AND EXECUTIVE OVERVIEW

Evidence is the basis of modern society. Since medieval times, concepts such as the burden of proof and the writ of *Habeas Corpus* have served as the foundation for our legal system.

Evidence is a tricky thing. In the early days of law, it was based on physical proof, or the testimony of witnesses under oath. It was inefficient, subject to tampering and destruction. Juries and judges had to consider not only the facts, but also the circumstances under which those facts were obtained and the trustworthiness of those testifying. They had to be very judicious.

All of that is changing. In the last twenty years, the human race has gone digital. In a digital world, evidence is dramatically different:

- It can be collected from many perspectives at virtually no cost.
- It can be stored and copied efficiently, without degrading the source material.
- It can be analyzed by machines, which can bring important facts to the forefront far more quickly than humans can and also find hidden patterns in data.
- It can be digitally signed, copied, and logged, providing a record of its use, preventing tampering, and reducing the chance of theft.

Collecting evidence is now a mainstream activity. We just don't call it evidence. We've embraced digital recording like never before. Storing our lives online—something that was unthinkable a decade ago—is now an everyday practice. We disclose what we're doing on Facebook, Twitter, Latitude, and Foursquare, uploading pictures and videos and updating our status constantly. The fight over our recorded lives is being fought in the blogs, headlines, and courtrooms of the nation.

Mobile devices are increasingly able to record our lives without direct intervention. The addition of GPS, cell-tower positioning, multitasking, and built-in cameras and microphones mean we are fast approaching a world in which we will record every part of our lives automatically.

The technical and cultural shifts that come from a digital life lived online will have dramatic implications for the legal systems on which society is based. Already, companies must keep digital records such as emails for use in civil and criminal investigations. What happens when humans must do the same?

TASER is well known as a maker of Less-Lethal Electronic Control Devices (LLECDs) used by law enforcement worldwide. Recently, however, they've branched into an adjacent market: collecting and recording digital evidence, using a capture device—dubbed AXON—and a hosted portal, [evidence.com](http://evidence.com)

There have been several well-documented tests of recording individual lives, from Gordon Bell's MyLifeBits project<sup>1</sup> at Microsoft to Sunil Vemuri's iRemember MIT

---

1 <http://research.microsoft.com/en-us/projects/mylifebits/>



thesis.<sup>2</sup> But broader initiatives like TASER's ongoing pilot projects with several police forces show us how groups of people react to an always-on, recorded environment.

Bitcurrent spent time with the team behind TASER's evidence.com project, looking at the state of evidence collection by police and the lessons learned during the rollout and trial of the technology by law enforcement personnel. TASER funded this report, but didn't exercise any editorial control—their goal was to open up the discussion about the recorded future of law enforcement to a wider audience. This report discusses those findings, and tries to anticipate what a recorded, searchable life will look like.

---

*While TASER provided us with considerable insight into their research and technology, the opinions expressed herein are those of Bitcurrent.*

---

---

<sup>2</sup> <http://web.media.mit.edu/~vemuri/wwit/wwit-overview.html>



## PART ONE: LIVING IN A RECORDED WORLD

---

The switch from analog to digital technology seems natural, because many of the things we do with digital data—watching television, listening to music, reading messages—are largely the same as their analog predecessors. But the switch to digital content has far-reaching consequences for humans: digital material doesn't degrade gradually, it can be searched and manipulated, it can be signed and verified, and it can be transmitted and copied indefinitely.

As we go about our lives, we're constantly shedding data. We send messages and emails. We use phones, leaving a trail of call records. We travel, marking our coordinates in GPS systems and bridge toll systems. We buy products with credit cards and loyalty points. We clear security systems. We don't think much about these activities. They're the by-products of living in a connected world. Our digital dandruff has always been a by-product of our day-to-day lives.

Recently, however, we've become more explicit about data collection. We update our status, share pictures with GPS coordinates, check in at venues, and upload videos for all to see. Rather than accidentally leaving a trail, we're plainly and openly blazing one for all to see.

### The merger of humans and technology

Phones, email, digital cameras, and social networks are part of our lives. Since the advent of the World Wide Web, connected consumer technology has insinuated itself into our cultural psyche.

One of the key reasons this has happened is that electronic devices have become both simpler and more complex. *Simpler*, because a broad segment of the market can use modern devices without much training. *More complex*, because the technology today far surpasses desktops only a few years old.

A modern smartphone incorporates audio/video capture and playback; GPS, compass, tower, and accelerometer positioning; powerful graphics; high-bandwidth Wifi and cellular data networking, gigabytes of storage, and more. It's the ideal extension of our capabilities, both in terms of recording a life and in terms of augmenting human consciousness—what Sunil Vermuri calls a *memory prosthesis*.

There are plenty of these prostheses out there. In 2009, consumers bought 170M smartphones. Nearly all had a built-in camera and audio recorder of some kind.<sup>3</sup> In April, 2010, Apple claimed that the 85M wireless devices it had sold accounted for 64 percent of America's mobile browsing. These kinds of devices work from almost anywhere. They're ubiquitous, blending in with the environment until they become unnoticeable. And they're culturally acceptable: commuters plug in to their mobile devices, oblivious to one another; partiers shoot pictures and videos constantly.

---

3 According to Maribel Lopez, Lopez Research.



## Cultural acceptance

We've accepted these devices. Not only are we familiar with them, but we're accustomed to viewing and sharing the information they produce. Many jurors understand a Facebook feed, or a video shot on a cameraphone, far better today than they did a few years ago. These new sources of data are a fact of life: consider that in 2009, 8% of companies over 1,000 people had dismissed an employee for improper use of a social network of some kind.

The change to a recorded life means the law is changing, too. In a number of high-profile cases, law enforcement has arrested citizens for recording them. Concerns over officer privacy run up against calls for accountability. Some states are applying wiretapping laws to public recordings of traffic stops and arrests, but what's clear is that the legal system didn't anticipate a world in which everyone was both able to record, and able to transmit that recording worldwide.



## PART TWO: RECORDING LAW ENFORCEMENT

---

### What does the right evidence do?

Having a valid record of what transpired has a huge impact on the effectiveness of law enforcement. For one thing, it stops false accusations: an IACP study showed that recorded evidence exonerated the officer 96 percent of the time. It increases the likelihood that an incident will lead to a charge or a summons: a 2007 study by the British Home Office showed that officer wearing headset recorders had a 47 percent increase in charges and summons. It also makes officers more productive: in the same study, those wearing the headsets spent 22 percent less time on paperwork, and roughly 50 minutes a day more on patrol.

### Getting tech in the precinct

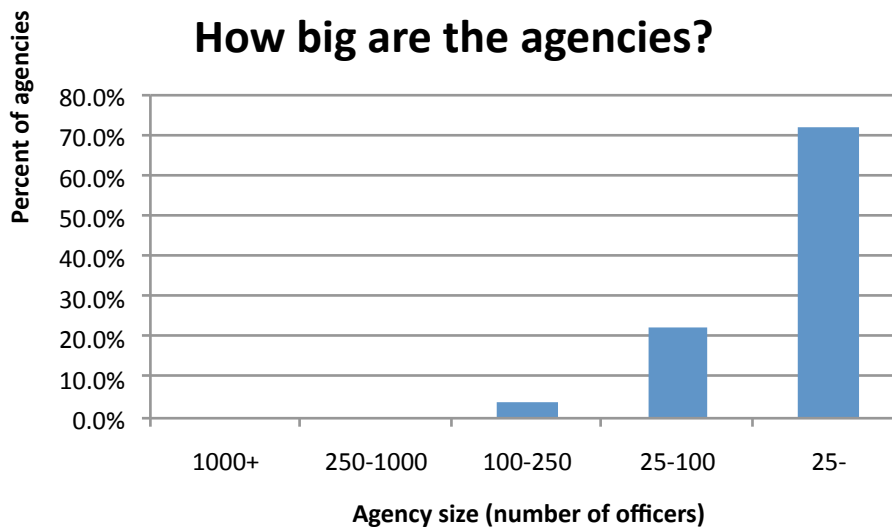
The challenge is getting reliable, legally admissible evidence collection into the hands of police officers. According to the U.S. Department of Justice, there are roughly 850,000 full-time law enforcement officers in the US today, from state and local police to campus police to federal employees in immigration, the FBI, the prison system, and border protection. Of these, roughly 700,000 are state and local law enforcement, of which 525,000 are regularly assigned patrol officers.

There are plenty of incidents for officers to capture. Roughly 130M incident reports are filed each year. 70M of them document new incidents, and roughly 200,000 of them (0.1 percent of all service calls) involve the use of force.

The largest police agencies file 2-3 use of force reports a day. Only 31 percent of local police agencies keep computer files on use-of-force incidents.

Patrol officers spend between 15 and 25 percent of their time writing incident reports, but the method they use to capture information varies by precinct and department, and may include dictation, typing, checklists, scanning, and laptop data entry. The vast majority of departments still use paper reporting and employ data clerks to transcribe information officers provide. While police forces and prosecutors rate video evidence as very effective in prosecution and exoneration, they report problems getting copies of evidence, redacting inadmissible portions of the evidence, maintaining a clear chain of custody, and providing defense attorneys with copies as part of disclosure and corroboration.

In other words, it's a decidedly low-tech, non-standardized environment. Most police departments in the U.S. have less than 25 sworn officers, and lack an in-house technical team to support sophisticated evidence management.



## How evidence is collected today

The radio is an officer's most important tool. It gives them more knowledge than their suspect, connects them with their peers, and allows them to work as a team. In the heat of the moment, it's often the most accurate record of what actually happened. This means two things:

- On-officer recording will succeed only when it becomes as essential as the radio system.
- Whatever recording tools are used must work alongside, rather than compete with, the radio on which the officer relies.

Law enforcement is already recording many of its activities when driving. In the U.S., police departments spend roughly \$500M a year on in-car recording and digital evidence management, but the vast majority—71 percent—of this is spent on the recording devices themselves. Storage, management, and analysis are an afterthought. Despite the focus on capture, companies like Digital Ally and Integrian have built solutions that are narrowly focused on the law enforcement market. There's a lot of demand: roughly 135,000 in-car recording devices need replacement, and over 300,000 cars have no in-car video. Most of the existing systems are analog, making the evidence they capture harder to process, copy, and handle.<sup>4</sup>

In-car video generates a huge amount of potential evidence, but it doesn't fit the way law enforcement personnel work. A 2004 study by the San Francisco Chronicle showed that roughly 90 percent of what police do happens away from their vehicle. A number of companies, like VIDMIC and VieVu, make on-body

<sup>4</sup> According to the U.S. DOJ Bureau of Justice Statistics (BJS) and the International Association of Chiefs of Police (IACP)



cameras, while others, including Robocam, Audax, Videovest, Tactical Electronics, and Maplin offer head-mounted models.

Besides the radio and the car, there are other ways to record events. Some devices (such as TASER's X-26 LLECD) can record the time and place at which they were discharged, and mobile phones log calls and can track coordinates from GPS or radio towers. Combine these offerings with the shrinking, increasingly powerful, PDA and it's clear that recording an officer's entire day isn't far off.

## Citizen media and its impact

The rise of citizen media—where every bystander is a potential contributor to the nightly news—means that every incident will be recorded by many people. Recording a video and posting it to sharing sites like Youtube is effortless, and officers will soon demand that their version of events gets an equal voice.

Recorded evidence isn't just good for productivity and exoneration. It's also an excellent way to defuse a situation, since both the officer and the subject behave better when they know their actions are being recorded. After-the-fact analysis of recorded metadata can reveal patterns of abuse: a San Francisco Chronicle investigation of use of force incidents between 1996 and 2004 showed that only 5 percent of officers were involved in 25 percent of incidents; ultimately, the city paid out over \$5M in force-related lawsuit settlements during that time.

## Connecting and computing

Simply recording information isn't the same as collecting evidence. Most police departments already store video on DVD or tape in huge warehouses. Unfortunately, retrieving and analyzing the right evidence is time-consuming, and the evidence itself is at risk of theft or damage.

An effective evidence system requires more than just capture and storage. It also needs:

- **In-the-field context.** Analyzing data after the fact is difficult, particularly if it lacks context. Capture solutions also have to let an officer add context—voice annotations, markers in the timeline, and so on—to make it easier to find and understand a particular portion of the evidence months or years later.
- **Search and filtering.** If officers are to make the best use of data, they have to be able to find specific records quickly, and jump to a particular incident. Technologies like voice transcription, motion detection, and facial recognition software can all point a prosecutor in the right direction.
- **Logging and workflow.** Evidence can become useless, or inadmissible, if it isn't properly controlled. Digital technologies such as encryption, signing, and logging can help provide the chain of evidence that juries require, reducing technicalities and ensuring that the record has its day in court.



- **Pivoting.** With several potential records of an event—including officer-captured data, radio transmissions, security footage, and user-generated content—investigators may want to pivot along several dimensions. Perhaps they want to see the same location from another person’s vantage point. Or they want to see the same place, a day earlier. Being able to pivot along several dimensions can yield new insights into what happened, much as Microsoft’s Photosynth technology can.

## How TASER’s system works

TASER’s system consists of two components: the AXON recording device, and the evidence.com portal. The AXON is a wearable computer connected to a head-mounted camera and the officer’s radio system, which captures a video of what happened during an incident in both regular and low-light-infrared forms.

Here’s how evidence makes its way from the street to the courtroom:

1. **At the start of a shift**, the officer enters their identification into the AXON, removes it from its charging system, and wears it. This assigns it to the officer.
2. **When an incident occurs**, the officer double taps recording button. The system maintains a 30-second buffer so that the officer can start recording retroactively, capturing how the incident began. As this happens, the AXON is collecting additional metadata such as location, movement, and weapon discharges automatically.
3. **If the officer needs to speak confidentially**, he or she can hit a “privacy” button to pause buffering temporarily. During this time, the fact that the system is not recording is clearly visible to others and the fact that the system was not recording is included in the evidence itself.
4. **After the incident**, the officer can review the recorded video, and annotate the record by voice or touchscreen keyboard to provide additional context and mark important events. While the device allows augmentation of the record, it does not allow the officer to delete it.
5. **At the end of their shift**, the AXON is docked to the charging system, which transmits all recordings to a secured storage facility (the “cop cloud”) run by TASER itself.
6. **Once uploaded**, the recording is processed in the cloud to augment the record—this is where technologies such as license plate matching and thumbnail generation of key events are used. Finally, it’s available through a Software-as-a-Service portal where it can be retrieved and analyzed.
7. **As part of their ongoing management of the precinct**, a supervisor can get an overview of all activity by all officers. The portal generates a map of incidents by location using the additional metadata collected by the device. It can search across metadata or track the movement of a particular group during an event.

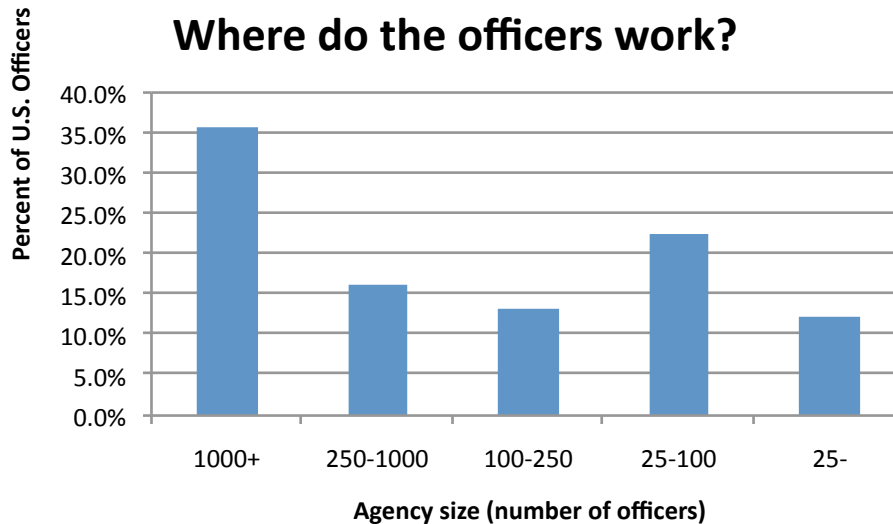


8. **In the course of an investigation**, many people—with the appropriate authorization—may access the evidence that was collected. This may include prosecutors, other officers, Internal Affairs investigators, or the officer themselves. Each of these accesses is logged as part of the evidence.



## PART THREE: THE CLOUD AND SAAS APPROACH

Earlier, we saw that most police departments are small. Yet the big ones are very, very large: the majority of officers work within large urban police departments.



Even among these larger precincts, there's little standardization for handling evidence, with much of the record-keeping still relying on analog video and paper incident reporting. Existing systems are unlikely to cope with the impact of officer- and citizen-generated evidence made possible by miniaturization and on-officer recording, and the lack of standardization inhibits cross-jurisdiction reporting and information sharing.

### The in-house versus SaaS model

In the past decade, the software industry has moved from a traditional licensing model—in which a customer buys a license to install and use software—to a Software-as-a-Service model. Companies like Salesforce.com have convinced even the largest companies to buy their software as a utility, paying a monthly fee in return for web access to an application.

It's a model that's familiar to consumers, who get everything from television to email to photo sharing as a hosted service. SaaS offerings work well when certain conditions exist:

- The user base is highly mobile, accessing information from many places
- Information in the system is shared by many people



- The end users are relatively non-technical, or don't want to invest in dedicated IT teams to run and maintain the software
- The application's features and functions are relatively standardized across all potential users, requiring little customization
- The infrastructure needed to run the system (storage, disaster recovery, bandwidth, security auditing, etc.) are expensive unless they're amortized across several customers.

These are some of the reasons why Salesforce.com and other salesforce automation products succeeded early in the SaaS industry: salespeople are mobile, share information, aren't very technical, and need the same basic functionality. Salesforce.com was able to achieve considerable economies of scale that no one customer could hope for.

SaaS is part of a larger movement in information technology known as *cloud computing*. Cloud computing involves automation, self-service, virtualization, and third-party operation of IT resources, and can reduce the time it takes to deploy systems significantly while at the same time offering "elasticity"—the ability to grow and shrink capacity as needed, because it's shared across many users.

One of the clear drivers for a hosted solution is the efficiencies of digital data. Police forces spend \$50M a year to handle and store videotapes. Each in-car camera costs \$600 in administration, and 81 percent of police forces catalog tapes by hand. 90 percent of those tapes are kept at police departments, often for months. Simply "going digital" hasn't helped. For many departments, digital has meant simply replacing videotapes with DVD media, which must still be physically stored and manually handled.

Given the specific needs of evidence processing, the lack of technical expertise, and the large number of small precincts, evidence collection and management is a good fit for a SaaS model. To make it work, however, TASER has had to overcome several challenges.

First, **video is hard to upload**. Uploading large video files from bandwidth-challenged departments can take a long time, and may require infrastructure upgrades. One solution is to cache the video locally, within the charging system, and upload it to hosted storage over time. This may introduce additional points of failure into the system, however, and raises the cost and complexity of the technology within the precinct itself.

Second, **processing takes time**. Even if the video is uploaded quickly, it takes time to transcode it, which doesn't fit in with the urgency of solving a case. Processing evidence to generate thumbnails, find faces, read license plates, and flag interesting moments requires tremendous computing power, and any analysis system must scale automatically to meet demand. Solutions like progressive playback—playing the video from the current cue point while transcoding backwards and forwards from that moment in time—can address these challenges.

Third, **video takes lots of storage**. Once it's been sent and analyzed, video needs to be stored. TASER has already seen officers recording their entire day, rather than



just incidents, and is revising its estimates for the amount of video generated by a department. The petabytes of online storage need a tiered architecture of immediate, delayed, and offline storage so that current cases can be accessed quickly while preserving evidence cost-effectively for the long term. Consider that 11,000 officers using a system such as TASER's would generate approximately 1.2 Petabytes of data, with 10 percent of that stored online for immediate access.

Fourth, **compliance is hard**. There's nothing more important than evidence itself. At first blush, sending sensitive material to a third party might seem risky; indeed, security is cited as one of the main fears companies have when adopting a cloud computing solution. In this case, however, clouds make the job easier. The current state of evidence management is manual, physical, and error-prone. Many people touch the evidence, from the officer to those transcribing, copying, and storing it. Moving to a digital, third-party model solves many of the problems with maintaining a chain of evidence by building logging and access control into the system itself, detecting data corruption when the evidence is first uploaded, handling requests for access to evidence, and preventing deletion of the evidence itself.



## PART FOUR: THE BUSINESS CASE FOR RECORDED ENFORCEMENT

The number of civil lawsuits filed against law enforcement professionals and the cities for which they work has grown dramatically in the last fifty years. A 1978 reversal by the U.S. Supreme Court declared municipalities “persons” that could be held vicariously liable for any act committed by an employee pursuant to a government policy or custom<sup>5</sup>, and the 1976 Attorney’s Fee Act encouraged a pattern of increased litigation, since prevailing plaintiffs’ attorneys could demand payment from defendants.

In 2009, the city of Chicago received 10,074 complaints about its officers, up 3% from 2008. The city’s Independent Police Review Authority opened up 9% more investigations than in the preceding year, a trend that continued in 2010. In New York City, claims of personal injury have doubled since 2001. According to the New York City Law Department, personal injury suits (which include everything from use of excessive force to false arrest to malicious prosecution) totaled 1,909 in 2009, and only 32% of them had been settled by May, 2010<sup>6</sup>. In 2007, the city received 7,559 complaints, each of which cost \$1,511 to resolve—\$317 per officer.

Investigating police wrongdoing is an expensive proposition. The cost of investigations alone makes recorded law enforcement a good investment, because it exonerates officers from false claims, while providing evidence of abuse when it occurs. A 1991 study across 165 agencies by the Journal of Criminal Justice found that 437 of the 3,515 officers in the study received complaints, and that 25% of these complaints were sustained, against 4.4% of the officers<sup>7</sup>.

Whatever the verdict, having a reliable record of what happened improves accountability and transparency, because administrators can review and demonstrate the inappropriate conduct so it can be dealt with promptly and fairly—further reducing the liability the municipality may incur.

There are other benefits from recording officers which are less immediate but perhaps more far-reaching:

- It **improves the behavior** of the officers and the civilian since both parties know they’re being recorded.
- Prosecution is easier when there’s a reliable, **indisputable chain of evidence**.
- Recorded systems can **reduce paperwork** and time spent documenting events, giving officers more time to patrol.

5       Lawsuits Against the Police: Reasons for the Proliferation of Litigation in the Past Decade, Alan Ray Stafford Sui Ross State University, Alpine, Texas (1986)

6       “Suits Against Police on the Rise”, Joel Stonington and Tom McGinty, Wall Street Journal, May, 2010

7       “Complaints about Police Officers: a comparison among types and agencies”, John R. Dugan and Daniel R. Breda, Journal of Criminal Justice, Vol. 19, pp 165-171 (1991)

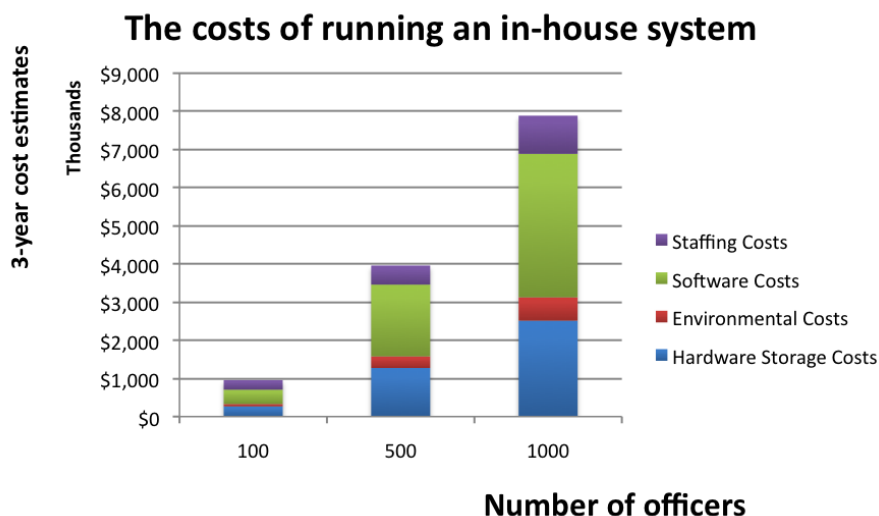


- Investigators can find clues in the recordings and **automate certain tasks**, such as video analysis, facial recognition, and license plate lookups.

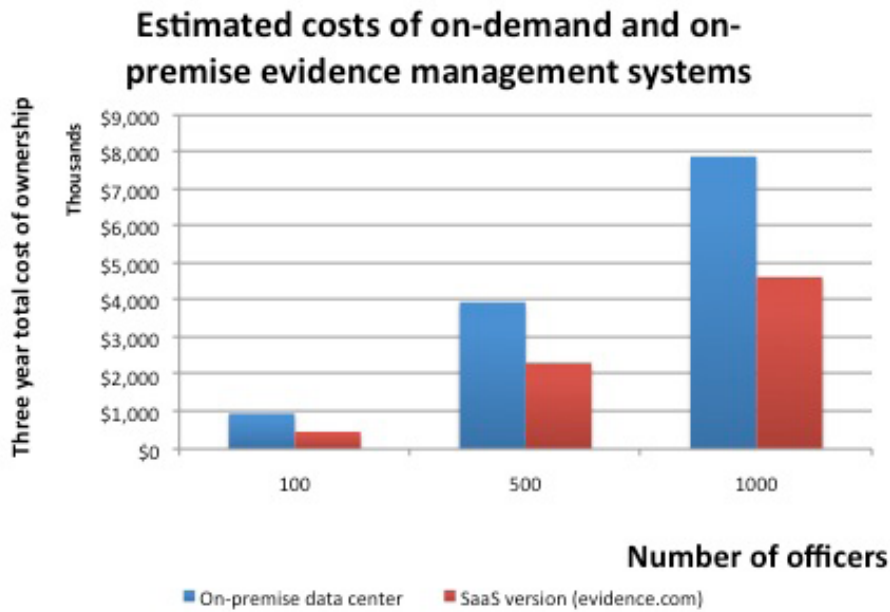
If we accept that recorded law enforcement is here to stay, then the question becomes: what's the best way to deliver it? Here, there are strong arguments for shared, multi-tenant platforms provided by a specialized service provider:

- There are economies of scale.** Massive amounts of computation, bandwidth, and storage—and the power, cooling, and physical infrastructure needed to support it—are beyond the capacity of law enforcement personnel in most areas. Focused service providers can locate their servers near power sources, negotiate for preferential land and facility rights, and constantly upgrade to take advantage of technical innovations.
- The storage model is unpredictable.** There will be network congestion at the end of a shift, as officers submit their recordings; processor congestion when transcoding new content; and competition for I/O resources increases when prosecutors are working with the evidence. A delay in any of these slows down the whole process; but having enough infrastructure to handle peak loads isn't cost-effective. Unpredictable workloads such as these need shared, on-demand, utility-based storage models.
- There are economies of skill, too.** It's not just sharing storage or processors—it's sharing expertise in certification, or audits, or security measures. Evidence is precious, and demands the most skilled curators to protect it.

It's hard to quantify the costs of implementing a recorded law enforcement strategy. TASER has analyzed the storage, staffing, and related costs of an in-house system, which vary according to the size of a precinct and the resulting data that's generated.



According to the company, their Evidence.com solution represents a roughly 30% savings versus on-premise recording alternatives.



In other words, for economic reasons alone, recorded law enforcement will probably become the norm in the near future; and those recordings will probably live in the cloud.



## PART FIVE: WHAT CAN WE LEARN FROM RECORDING EVERYTHING?

Whether we're talking about Evidence.com or Flickr, the key elements of a recording system are:

- The capture of the event, along with automatic metadata, including a retro-recording when the camera is activated
- *Annotation and context* provided at the time
- *Additional information* provided after the fact
- The *machine augmentation* that occurs within the cloud
- *Search, filtering, visualization*, and pivoting that can be done across several streams of data
- *Logging and permissions* associated with access to that information.

These elements exist whether we're talking about formal evidence capture, or about a less heavily-regulated form of data collection. Consider a photo uploaded to Flickr, for example:

- When we take a photograph with a camera, the make, model, time, and date are stored.<sup>8</sup>
- If the camera includes the feature, we can record a small audio clip describing the image by pressing a button on the camera itself
- We run Flickr's "uploadr" tool and add information, tagging people in each picture and editing descriptions.
- Flickr receives the image, generating thumbnails and performing photo optimization to enhance colors.
- Flickr's interface lets us search across our photos and those of others by tags, time, camera, and other metadata. It offers a variety of visualizations, from thumbnails to calendars to timelines, to make it easier to find and display the right image.
- Flickr keeps track of how frequently each picture has been taken.

There are many important lessons to be learned from these examples.

### Cloud computing allows the system to handle spikes

What makes solutions like this possible isn't just the capture device—indeed, capture will soon be ubiquitous. It's the cloud computing platforms on which

---

<sup>8</sup> Unfortunately, because we're not recording everything, we miss many great pictures. As video resolution and storage capacity approach that of digital cameras, we'll likely opt to record everything in a buffer just in case.



they depend. Evidence.com is a shared, elastic computing resource. That makes it economical where local approaches would fail.

Any given police department's use of the system is unpredictable. That is, there are periods of heavy use and periods of idleness. At the end of a shift, everyone's uploading content; during the day, investigators are accessing evidence. By sharing the computing resources across many departments, TASER can achieve greater economies of scale and skill than an individual precinct could.

## Context is everything

In the heat of the moment, it's unlikely that an officer will devote any attention to annotating and augmenting a recording. That means the system needs to do it for them. The more context that a recording system can capture—from accelerometer data showing rapid deceleration, to timing data that allows investigators to line up multiple perspectives from several officers—the better the quality of the evidence and the more that can be done with it.

Eventually, multiple concurrent recordings become a new kind of evidence. Given enough simultaneous views, it'll be possible to re-create crime scenes after the fact much as Photosynth can render famous landmarks from the many photographs taken by tourists.

Whether we're talking about the Evidence.com example or the Flickr example, most of the work isn't the capture itself—it's the augmentation, annotation, search, and visualization. As more and more of our digital lives are stored online, finding what we're looking for becomes increasingly challenging. So it is with evidence: the deluge of incident information that police precincts are about to experience isn't about capturing more information, it's about making that information more accessible and contextual.

## Moving across dimensions

Every piece of metadata captured by a recording system becomes a way to pivot across dimensions. In the Flickr example above, a picture has metadata—the camera make and mode, the time, the location, the people tagged in the picture, the dominant color. Each of these is a dimension along which an analyst can pivot, finding other pictures taken at the same place, or featuring the same people. This pivoting behavior will become an integral part of building a case, but it'll also be a natural way to browse through all kinds of digital information. Metadata is less about finding a particular piece of evidence, and more about relating it to other pieces in ways that reveal patterns.

## Everything will be recorded

The ability to be “always potentially recording” is essential. You never know what will be interesting until it's already happening. It's likely that buffering of this sort will become commonplace in all manner of lifestreaming and data collection systems, rather than just in security systems. What's more, early feedback from police trials



suggest that some officers leave the device recording at all times, which makes data processing difficult but means that everything is captured.

## Digital, shared systems make network effects possible

Having a single copy of evidence makes it hard to share information. But when that evidence is digital, great things happen. It can be shared across users (assuming the right permissions are in place) and compared side-by-side. Having fifteen different perspectives of a single event will let investigators build a more immersive model of what took place at the crimescene.

Simply showing what else happened at a given place and time is a massive step, and centralized records means machines can prompt humans to connect the dots. A particular investigator may not have access to related data—but a machine can suggest related information that others control, prompting them to collaborate. With the help of machines, cross-user cooperation might become a reality. IBM's researchers are already employing predictive analytics to fight crime, and believes that it will become a multi-billion-dollar market.<sup>9</sup>

As consumers adopt similar technologies, sharing and mashing together records of what happened will become more common. Imagine that a thousand people synchronize their watches, gather in Times Square, then record five minutes of video on their phones. Knowing the position and location of each phone, we can build an immersive 3D view of what happened, allowing the viewer to navigate in both time and space within those five minutes.

With digital evidence, we'll realize that multiple records of an incident, captured by officers, security cameras and citizens—then linked by the right metadata—has transformed law enforcement. The growth of user-generated content will change the way laws are enforced. It's a "Majority Report", in which a preponderance of evidence, backed by the power of rich analytics, changes how we determine guilt.

## Moving from one-way to two-way

While TASER's current offering is one-way, it's not hard to see what a two-way system would look like. By combining recording capabilities with augmented reality, three kinds of sharing occur:

- Between the officer and the record of evidence, using the capture systems described above
- Between one officer and another, in real time. This tactical use of information might superimpose what several officers are seeing during an incident, allowing one officer to see through a wall or a perpetrator and identify a weapon

<sup>9</sup> <http://trueslant.com/daviddisalvo/2010/04/17/ibms-crime-prediction-tech-makes-profiling-seem-like-childs-play/>



- Between the department's information resources and the officer—overlaying traffic violations on vehicles, or showing registered firearms holders as an officer drives through a neighborhood

The impediments to this kind of two-way, tactical offering are significant. They mustn't interfere with the officer's work, or put him at risk. They require low-latency, high-bandwidth, two-way networking, both locally and between the officer and the central data store. And they must resist attacks and tampering that might incapacitate the officer. But these challenges can be solved with emerging high-speed wireless networking, good design, and many other emerging technologies.

## Cameras don't need to swear oaths

A digital record eliminates the need for anecdotal evidence. At the same time, juries are ready to accept information from digital sources; they've been trained by the Web, Facebook, iTunes Coverflow, Google Earth, and many other technical interfaces that are now commonplace. Ultimately, court cases will hinge not on the raw evidence—there will simply be too much of it to consume—but on who has the best tools to analyze it and present it succinctly.

Many organizations are already focusing on rules and standards for the management of digital evidence: the Law Enforcement & Emergency Services Video Association ([leva.org](http://leva.org)), the Scientific Working Group on Digital Evidence ([swgde.org](http://swgde.org)), the International Association for Identification ([theiai.org](http://theiai.org)), and the National Incident Management System (NIMS).



## CONCLUSIONS

Many of the technologies and trends we've covered won't just apply to law enforcement personnel, however. They'll also change how criminals and law-abiding citizens interact with law enforcement officers.

It's no longer about who has the recording of a conflict—it's about who's able to make the most of that recording, with access to analysis, processing, and correlation tools.

The simple knowledge that one is being recorded can change behaviors; and as a society we need to decide whether recording and broadcasting is equivalent to free speech, and what expectations of privacy participants in that conversation enjoy. Whether tomorrow is an idealistic utopia of accountability or an Orwellian dystopia of state surveillance, the trends are moving towards video evidence.

Ultimately, the shift to digital, hosted evidence management will transform how our legal system works, shifting the burden of proof and creating an expectation of evidence. A convergence of digital capture, metadata and annotation, chain-of-evidence tracking, and powerful cloud-based analytics and visualization paint a compelling picture of tomorrow's police officer.

There are significant ethical and legal issues that voters and courts must untangle in the era of prosthetic memory. But one thing is clear: a recorded world is here to stay, and the tools to analyze that world will become an integral part of the legal process.



## ABOUT BITCURRENT

Since 2006, Bitcurrent has been covering emerging technologies with a focus on web performance, cloud computing, and next-generation applications. We publish primary research, run the industry's largest cloud events, and advise investors, technology firms, and private and public sector organizations on their IT strategy.

This report is distributed according to a Creative Commons Attribution/Share Alike license. You are free to share (copy, distribute and transmit the work) and remix (to adapt the work) provided that you include attribution to [www.bitcurrent.com](http://www.bitcurrent.com) and that any resulting works are distributed under the same license—that is, that others may share and remix your work.

**[www.bitcurrent.com](http://www.bitcurrent.com)**  
**[info@bitcurrent.com](mailto:info@bitcurrent.com)**  
**1-888-796-8364**

