The Daily Beast

SHOOTERS 09.11.14

Jacob Siegel

Your Arrest Video Is Going Online. Who Will See It?

America is rushing to outfit cops with cameras, but even experts aren't sure of the laws regulating the storage of the videos they capture—or determining who exactly has access.

In the aftermath of Ferguson, where the death of an unarmed teenager sparked weeks of protests, police departments across America are outfitting their officers with wearable cameras. The devices themselves raise plenty of legal and privacy questions, but ever bigger issues loom about what happens after they are shut off.

Police departments are already outsourcing their video evidence to private companies, creating problems so knotty and new that even the ACLU doesn't have answers for them. Among them:

• How long will evidence be stored, and how will police departments verify the information has actually been wiped after its supposed deletion date?

• Will federal law enforcement and intelligence agencies like the FBI and NSA need warrants and subpoenas to view the digital evidence in private companies' cloud storage? And will they deal with local police departments or go directly to the private storage services?

• Will the public get to see the police footage, for example, when there is evidence of misconduct?

• What happens when a private company's server is hacked and evidence is lost or compromised?

Think of it like this: The police will have moved their evidence into a private warehouse staffed by private security guards and administrators. These private guards can see the boxes the evidence is stored in, how many and when they come in, but they're not supposed to look inside. And instead of only keeping evidence related to criminal matters, this private warehouse is storing a bottomless pit of routine interactions between cops and citizens. Going 50 in a 35? Got stopped because you fit the description, but quickly released once the cops realized you weren't the person they were looking for? There's going to be a video of you in a private corporation's digital records.

This isn't abstract. In Michael Brown's case, outrage that the teenager's fatal shooting wasn't recorded was paired with a video released by Ferguson Police Chief Thomas Jackson, showing the teen appear to push a clerk and leave a store with a box of unpaid-for cigars. It shortly emerged that the officer who shot him had no knowledge of that earlier crime, and many accused the police chief of releasing the video to smear a dead man. The same massive evidence trove body cameras create can, if used selectively, humiliate and indict average citizens.

Making all this even more complicated, the police cameras seem to work. They haven't been in use long enough or widely enough for a comprehensive study, but early results show that when cops wear them both police use of force and civilian complaints against officers drop substantially.

That helps explain why some of the loudest voices in support of cameras, such as New York Public Advocate Tish James, are coming from people usually suspicious of police power. In New York, the issue came to the forefront this summer after a bystander recorded video of police fatally choking an unarmed civilian. A growing chorus is touting the cameras as the answer to the complex issues of police violence and accountability, but a small group in the back of the room is worrying about the problems of outsourcing a modern panopticon even as it's getting constructed.

What conversation is occurring about transparency and the public interest is mostly happening in private, and between government officials and the companies selling them products.

Despite early reservations, New York's police force, the nation's largest, is following smaller departments and adopting cameras for some of its 35,000 officers. The cameras are being introduced as part of a pilot program but they represent "the next wave" in police technology, according to NYPD Police Commissioner William Bratton, who compared the devices to walkie-talkies.

The big unanswered question, Bratton said, is what to do with all the video footage captured by the cameras. "The amount of information one device can accumulate in the course of several hours in a day; the cost of storing it; how to retrieve it—these are not simple issues to resolve," Bratton told a group of reporters.

The answer many departments are turning to is private storage. One company is becoming the market leader as the virtual evidence room for local police—Evidence.com. A subsidiary of Taser International, which also sells the AXON series body cameras marketed to police departments, Evidence.com promises to "collect, transfer, manage, retrieve, and share any form of digital evidence," according to its website.

The company has weathered controversies and a series of lawsuits over deaths attributed to its supposedly non-lethal tasers, but lately business has been looking up. On the strength of its body cameras and storage service, offered together as a package deal, Taser's stock has been rising, up 11.4 percent so far this year and projected to continue climbing.

Traditionally, police evidence has been kept under strict supervision in a property room, where authorized officers have to check it in and sign it out. Digital evidence like video has typically been stored as a hard copy, either on tape or DVD, and maintained under the same standards. That level of supervision protected the chain of custody and ensured that evidence wasn't lost, tampered with, or used for unofficial purposes.

Evidence.com offers its own protections, including authenticating users and providing an audit log detailing whenever users access digital files. Instead of a lock and key, you get "strong encryption to protect evidence data in transit and at rest." In place of a human guard, Taser offers "multiple multi-factor authentication options" and the ability to "restrict access to defined IP ranges."

Still, "police agencies have spent more than a century building bunkers to store and protect physical evidence and have adopted strict controls," Lt. Vern Sallee of California's Chula Vista Police Department wrote in an industry paper about "Moving Digital Evidence to the Cloud." The digital evidence room, in contrast, has only been around for a few years, meaning that Evidence.com is working out its real-world procedures on the fly, as business comes in. Like many Web services, it's effectively using police departments as beta testers for its product.

> More cameras are hitting the streets, Taser's stock is rising, and the digital evidence is already piling up—but the public scrutiny and regulation have been lagging behind.

So far there are no federal regulations regulating the private evidence cloud. Even at the state level, it's not always clear how laws written with pen and paper will apply to the virtual sphere. "States could impose different obligations on companies but under federal law there aren't really restrictions on how the data is safeguarded, how long it can be retained, or anything like that, " said Hanni Fakhoury, staff attorney for the Electronic Frontier Foundation (EFF). Evidence.com didn't answer a question about whether it works with any federal law-enforcement agencies, but the lack of federal statutes could be a problem if it does.

"The security and privacy issues about using third parties to store data is the same with any third-party vendor that stores data," Fakhoury said. A partial rundown of the issues Fakhoury cited: "Are they keeping it secure from unauthorized access? Are they working with the departments to retain only the amount of security footage absolutely necessary for police work? Are the third-party vendors mining this data for other purposes? Running analytics on it?"

"Fundamentally," Fakhoury concluded, "these are important questions that require public transparency." More cameras are hitting the streets, Taser's stock is rising, and the digital evidence is already piling up—but the public scrutiny and regulation have been lagging behind.

Evidence.com public relations director Sydney Siegmeth acknowledges that the company performs some analysis on the data it stores, but called it "the typical business measurements that a [Storage-as-a-Service] would run to track the health and performance of their business." Siegmeth said Evidence.com employees "don't, however, have access to our customers' data, as they own the data and unless they escalate to our support team and grant us access to resolve support-related issue, we don't see it. All access is audited." The answer suggests that the company doesn't peer into the video itself but tracks the circumstantial data associated with videos—i.e. how often a particular video is viewed, and by whom.

To be sure, there's no indication that Evidence.com is doing data mining in the way we associate with Facebook or Google—combing through user information to target clients with products—but the limits on what they can do appear to largely be set by the company itself.

One fundamental question that Taser declined to answer: What happens when a federal agency wants access to evidence it is storing? What if, say, the FBI wants to look through video of political protests? Or what if a district prosecutor with authorized access used the site to copy footage from a political opponent's arrest for public intoxication? That's a particularly relevant example given that the cloud service allows a user to "add your DA as a user to EVIDENCE.com account so that he/she can review videos from their office."

The presumption is that any non-authorized user, even a federal law enforcement agent, would need a subpoena to view footage, but even legal experts couldn't say for sure.

"The whole technology is so new there are only a few experts in it. We're really in the very early days still," said the ACLU's Jay Stanley, who counts among the few experts on the subject but expressed uncertainty about how Fourth Amendment protections and disclosure requirements would be applied to a third party hosting digital evidence.

"State and local government statutes govern the policy around how evidentiary data is stored and managed," Evidence.com's Siegmeth said. So, for example, one police department may have any evidence not involved in an open investigation deleted after 90 days, while another department may keep it for 180 days. When that period expires, Evidence.com deletes the data and "the police department would receive an email notification and the action would be recorded in the audit log."

Even "destroyed" becomes an uncertain term when applied to these sort of digital files. The actual video of a police incident may be deleted at the date set by the department, but some record of it appears to stay in Evidence.com's system. When asked, "Is metadata retained after video files are destroyed?" Siegmeth's reply was ambiguous. "We have a detailed audit system that tracks the life cycle of an evidentiary item for record-keeping purposes," she said.

The ACLU's Jay Stanley was unsure of how the law would be applied in cases where federal agencies wanted access to digital files hosted by Evidence.com. "These are really good questions," Stanley said, "and I don't know the answers to them."

If Stanley and other legal experts are unsure, it's a safe bet the public doesn't have an informed opinion yet and the matter might require more debate before cameras become a standard part of the police uniform and the cloud starts overflowing with video files.

Weighed against the bodies of unarmed civilians, warnings about the dangers of surveillance technology haven't created much resistance. Even the ACLU, which supports the cameras "as a check against the use of power by police officers," cautions that without sufficient regulatory policies their "benefits would not exceed their privacy risks."

Taser isn't the only company selling body cameras to police and it won't be the only one offering to host their data for long. Calculating the balance between risk and benefit and setting clear standards now could set an important precedent before other companies crowd the market and even more law enforcement footage gets entrusted to private guards.

The attitude so far has been to get the cameras out on the streets and worry about the policy issues later. As we learned—or should have—with the NSA, that's a dangerous way to do business.

According to Stanley of the ACLU, "The most common thing that happens is the police just buy them and start using them, often with very little protection for privacy at all."