Police Body-Mounted Cameras: With Right Policies in Place, a Win For All

By Jay Stanley, ACLU Senior Policy Analyst
October, 2013

Introduction[1]

When a New York judge found that the NYPD's stop and frisk tactics violated the constitutional rights of New Yorkers, one of the remedies she ordered was for the department to begin testing wearable police cameras, sparking debate and discussion of the technology there.

These "on-officer recording systems" (also called "body cams" or "cop cams") are small, pager-sized cameras that clip on to an officer's uniform or sunglasses or are worn as a headset, and record audio and video of the officer's interactions with the public. We have heard reports of police body cameras being deployed in numerous cities, and one prominent manufacturer told NBC that it had sold them to "hundreds of departments."

The ACLU has commented on police body cameras in the media several times over the years (and in stories surrounding the stop and frisk ruling), but the ACLU's views on this technology are a little more complicated than can be conveyed through quotes in a news story.

Although we generally take a dim view of the proliferation of surveillance cameras in American life, police on-body cameras are different because of their potential to serve as a check against the abuse of power by police officers. Historically, there was no documentary evidence of most encounters between police officers and the public, and due to the volatile nature of those encounters, this often resulted in radically divergent accounts of incidents. Cameras have the potential to be a win-win, helping protect the public against police misconduct, and at the same time helping protect police against false accusations of abuse.

We're against pervasive government surveillance, but when cameras primarily serve the function of allowing public monitoring of the government instead of the other way around, we generally regard that as a good thing. While we have opposed government video surveillance of public places, for example, we have supported the installation of video cameras on police car dashboards, in prisons, and during interrogations.

At the same time, body cameras have more of a potential to invade privacy than those deployments. Police officers enter people's homes and encounter bystanders, suspects, and victims in a wide variety of sometimes stressful and extreme situations.

For the ACLU, the challenge of on-officer cameras is the tension between their potential to invade privacy and their strong benefit in promoting police accountability. Overall, we think they can be a win-win—but *only* if they are deployed within a framework of strong policies to ensure

[1] The author would like to thank Doug Klunder of the ACLU of Washington, who did much of the thinking behind the analysis set forth in this paper; Scott Greenwood of Ohio; and his colleagues at the national office, for their valuable feedback and advice.

they protect the public without becoming yet another system for routine surveillance *of* the public, and maintain public confidence in the integrity of those privacy protections. Without such a framework, their accountability benefits would not exceed their privacy risks.

On-officer cameras are a significant technology that implicates important, if sometimes conflicting, values. We will have to watch carefully to see how they are deployed and what their effects are over time, but in this paper we outline our current thinking about and recommendations for the technology. These recommendations are subject to change.

Control over recordings

Perhaps most importantly, policies and technology must be designed to ensure that police cannot "edit on the fly" — i.e., choose which encounters to record with limitless discretion. If police are free to turn the cameras on and off as they please, the cameras' role in providing a check and balance against police power will shrink and they will no longer become a net benefit.

The primary question is how that should be implemented.

Purely from an accountability perspective, the ideal policy for body-worn cameras would be for continuous recording throughout a police officer's shift, eliminating any possibility that an officer could evade the recording of abuses committed on duty. Of course, just as body cameras can invade the privacy of many innocent citizens, continuous deployment would similarly impinge on police officers when they are sitting in a station house or patrol car shooting the breeze — getting to know each other as humans, discussing precinct politics, etc. We have some sympathy for police on this; continuous recording might feel as stressful and oppressive in those situations as it would for any employee subject to constant recording by their supervisor. True, police officers with their extraordinary powers are not regular employees, and in theory officers' privacy, like citizens', could be protected by appropriate policies (as outlined below) that ensure that 99% of video would be deleted in relatively short order without ever being reviewed. But on a psychological level, such assurances are rarely enough. There is also the danger that the technology would be misused by police supervisors against whistleblowers or union activists — for example, by scrutinizing video records to find minor violations to use against an officer.

If the cameras do not record continuously, that would place them under officer control, which would create the danger that they could be manipulated by some officers, undermining their core purpose of detecting police misconduct. This has sometimes been an issue with patrol car "dashcams" — for example, in the case of two Seattle men who filed a claim for excessive force and wrongful arrest. Parts of the arrest were captured by a dashcam, but parts that should have been captured were mysteriously missing. And with body cams, two Oakland police officers were disciplined after one of the officers' cameras was turned off during an incident.

The balance that needs to be struck is to ensure that officers can't manipulate the video record, while also ensuring that officers are not subjected to a relentless regime of surveillance without any opportunity for shelter from constant monitoring.

One possibility is that some form of effective automated trigger could be developed that would allow for minimization of recording while capturing any fraught encounters — based, for example, on detection of raised voices, types of movement, etc. When it comes to dashcams,

the devices are often configured to record whenever a car's siren or lights are activated, which provides a rough and somewhat (though not entirely) non-discretionary measure of when a police officer is engaged in an encounter that is likely to be a problem. That policy is not applicable to body cams, however, since there is no equivalent to flashing lights. And it's not clear that any artificial intelligence system in the foreseeable future will be smart enough to reliably detect encounters that should be recorded. In any case, it is not an option with today's technology.

If a police department is to place its cameras under officer control, then it must put in place tightly effective means of limiting officers' ability to choose which encounters to record. That can only take the form of a department-wide policy that mandates that police turn on recording during every interaction with the public.

And this requirement must have some teeth associated with it — not only a risk of disciplinary action but also perhaps an exclusionary rule for any evidence obtained in an unrecorded encounter (for police who have been issued the cameras, unless there is an exigency to justify the failure to record). Another means of enforcement might be to stipulate that in any instance in which an officer wearing a camera is accused of misconduct, a failure to record that incident would create an evidentiary presumption against the officer.

Limiting the threat to privacy from cop cams

Most of the discussion around police recording has focused on its oversight potential. But that is only one of the significant interests implicated by recording. Equally important are the privacy interests and fair trial rights of individuals who are recorded. Ideally there would be a way to minimize data collection to only what was reasonably needed, but there's currently no technological way to do so.

Police body cameras mean that many instances of entirely innocent behavior (on the part of both officers and the public) will be recorded, with significant privacy implications. Perhaps most troubling is that some recordings will be made inside people's homes, whenever police enter — including in instances of consensual entry (e.g., responding to a burglary call, voluntarily participating in an investigation) and such things as domestic violence calls. In the case of dashcams, we have also seen video of particular incidents released for no important public reason, and instead serving only to embarrass individuals. Examples have included DUI stops of celebrities and ordinary individuals whose troubled and/or intoxicated behavior has been widely circulated and now immortalized online. The potential for such merely embarrassing and titillating releases of video is significantly increased by body cams.

Therefore it is vital that any deployment of these cameras be accompanied by good privacy policies so that the benefits of the technology are not outweighed by invasions of privacy. The core elements of such a policy follow.

Notice to citizens

Most privacy protections will have to come from restrictions on subsequent retention and use of the recordings. There are, however, a couple of things that can be done at the point of recording.

1) Recording should be limited to uniformed officers and marked vehicles, so people know what to expect. An exception should be made for SWAT raids and similar planned uses of force when they involve non-uniformed officers.
2) Officers should be required, wherever practicable, to notify people that they are being recorded (similar to existing law for dashcams in some states such as Washington). One possibility departments might consider is for officers to wear an easily visible pin or sticker saying "lapel camera in operation" or words to that effect.
3) Although if the preceding policies are properly followed it should not be possible, it is especially important that the cameras not be used to surreptitiously gather intelligence information based on First Amendment protected speech, associations, or religion.

Recording in the home

Because of the uniquely intrusive nature of police recordings made inside private homes, officers should be required to be especially sure to provide clear notice of a camera when entering a home, except in circumstances such as an emergency or a raid. Departments might also consider a policy under which officers ask residents whether they wish for a camera to be turned off before they enter a home in non-exigent circumstances. (Citizen requests for cameras to be turned off should themselves be recorded to document such requests.) Cameras should never be turned off in SWAT raids and similar police actions.

Retention

Data should be retained no longer than necessary for the purpose for which it was collected. For the vast majority of police encounters with the public, there is no reason to preserve video evidence, and those recordings therefore should be deleted relatively quickly.

- Retention periods should be measured in weeks not years, and video should be deleted after that period unless a recording has been flagged. Once a recording has been flagged, it would then switch to a longer retention schedule (such as the three-year period currently in effect in Washington State).
- These policies should be posted online on the department's website, so that people who have encounters with police know how long they have to file a complaint or request access to footage.
- Flagging should occur automatically for any incident:
    - involving a use of force;
    - that leads to detention or arrest; or
    - where either a formal or informal complaint has been registered.
- Any subject of a recording should be able to flag a recording, even if not filing a complaint or opening an investigation.
- The police department (including internal investigations and supervisors) and third parties should also be able to flag an incident if they have some basis to believe police misconduct has occurred or have reasonable suspicion that the video contains evidence of a crime. We do not want the police or gadflies to be able to routinely flag all recordings in order to circumvent the retention limit.
- If any useful evidence is obtained during an authorized use of a recording (see below), the recording would then be retained in the same manner as any other evidence gathered during an investigation.

- Back-end systems to manage video data must be configured to retain the data, delete it after the retention period expires, prevent deletion by individual officers, and provide an unimpeachable audit trail to protect chain of custody, just as with any evidence.

Use of Recordings

The ACLU supports the use of cop cams for the purpose of police accountability and oversight. It's vital that this technology not become a backdoor for any kind of systematic surveillance or tracking of the public. Since the records will be made, police departments need to be subject to strong rules around how they are used. The use of recordings should be allowed only in internal and external investigations of misconduct, and where the police have reasonable suspicion that a recording contains evidence of a crime. Otherwise, there is no reason that stored footage should even be reviewed by a human being before its retention period ends and it is permanently deleted.

Subject Access

People recorded by cop cams should have access to, and the right to make copies of, those recordings, for however long the government maintains copies of them. That should also apply to disclosure to a third party if the subject consents, or to criminal defense lawyers seeking relevant evidence.

Public Disclosure

When should the public have access to cop cam videos held by the authorities? Public disclosure of government records can be a tricky issue pitting two important values against each other: the need for government oversight and openness, and privacy. Those values must be carefully balanced by policymakers. One way to do that is to attempt to minimize invasiveness when possible:

- Public disclosure of any recording should be allowed with the consent of the subjects, as discussed above.
- Redaction of video records should be used when feasible — blurring or blacking out of portions of video and/or distortion of audio to obscure the identity of subjects. If recordings are redacted, they should be discloseable.
- Unredacted, unflagged recordings should not be publicly disclosed without consent of the subject. These are recordings where there is no indication of police misconduct or evidence of a crime, so the public oversight value is low. States may need to examine how such a policy interacts with their state open records laws.
- Flagged recordings are those for which there is the highest likelihood of misconduct, and thus the ones where public oversight is most needed. Redaction of disclosed recordings is preferred, but when that is not feasible, unredacted flagged recordings should be publicly discloseable, because in such cases the need for oversight outweighs the privacy interests at stake.

Good technological controls

It is important that close attention be paid to the systems that handle the video data generated by these cameras.

- Systems should be architected to ensure that segments of video cannot be destroyed. A recent case in Maryland illustrates the problem: surveillance video of an incident in

which officers were accused of beating a student disappeared (the incident was also filmed by a bystander). An officer or department that has engaged in abuse or other wrongdoing will have a strong incentive to destroy evidence of that wrongdoing, so technology systems should be designed to prevent any tampering with such video.

- In addition, all access to video records should be automatically recorded with immutable audit logs.
- Systems should ensure that data retention and destruction schedules are properly maintained.
- It is also important for systems be architected to ensure that video is only accessed when permitted according to the policies we've described above, and that rogue copies cannot be made. Officers should not be able to, for example, pass around video of a drunk city council member, or video generated by an officer responding to a call in a topless bar, or video of a citizen providing information on a local street gang.

It is vital that public confidence in the integrity of body camera privacy protections be maintained. We don't want crime victims to be afraid to call for help because of fears that video of their officer interactions will become public or reach the wrong party. Confidence can only be created if good policies are put in place and backed up by good technology.

As the devices are adopted by police forces around the nation, studies should be done to measure their impact. Only very limited studies have been done so far. Are domestic violence victims hesitating to call the police for help by the prospect of having a camera-wearing police officer in their home, or are they otherwise affected? Are privacy abuses of the technology happening, and if so what kind and how often?

Although fitting police forces with cameras will generate an enormous amount of video footage and raises many tricky issues, if the recording, retention, access, use, and technology policies that we outline above are followed, very little of that footage will ever be viewed or retained, and at the same time those cameras will provide an important protection against police abuse. We will be monitoring the impact of cameras closely, and if good policies and practices do not become standard, or the technology has negative side effects we have failed to anticipate, we will have to reevaluate our position on police body cameras.