What Body Camera Data Should Police Collect and When?

pio3 / Shutterstock.com

These questions should be answered at the time of BWC deployment.

BY NELSON BUNN AND BRYAN CUNNINGHAM, CONTRIBUTORS | OCTOBER 15, 2015

In the first article (http://www.routefifty.com/2015/09/police-body-camera-musts/121502/) of our three-part series on widespread deployment of body-worn cameras (BWCs) by law enforcement, we argued that policymakers and law enforcement leaders face a broad and complex set of decisions that must be made now.

These vital decisions divide into the same basic categories as most big data or technology policy questions:

- collection and analysis of data;

- storage (including cloud storage), disclosure and retention or destruction of data;

- and secondary use and repurposing of data.

As our second article of this series, we consider the most important collection issues that must be decided immediately upon BWC deployment, in order to forestall complex problems down the line.

Collection of Data

While there are important economic and compatibility decisions to be made in purchasing BWCs themselves, the tough problems really begin when the cameras are turned on and petabytes of video, and potentially audio, data begin to stream into servers located at law enforcement agencies and in the cloud.

Video Only or Audio Too?

Under US law, and in most western democracies, video recordings are considered to be less privacy-sensitive than audio recordings and for good reason: While video recordings certainly can reveal private, even

embarrassing, information about individuals and their behavior, recordings of statements and conversations can be far more intrusive.

Anecdotal evidence suggests that at least some law enforcement agencies in the United States are opting, almost by default and likely without a thorough decision-making process, to record audio as well as video via BWCs. We understand this temptation; it enables a fuller record, may capture confessions and other valuable evidence, and provides fuller context that may protect law enforcement officers from false allegations of misconduct, as well as innocent persons against wrongful convictions.

However, we are not certain this is the wisest outcome, particularly if the audio is “always on” (see below).

First, under some circumstances, consent may be required, or at least advisable, for police to record audio of those with whom they interact or, at a minimum, police may need to provide clear and unambiguous notification to those being recorded.

Second, while there are valid reasons for law enforcement to record statements of victims, witnesses and, upon constitutionally-required warnings in some circumstances, suspects, are we better off as a society if law enforcement records *all verbal interactions with all individuals* with whom they come into contact? This would include people asking directions, citizens in physical or mental distress and many others not directly related to any criminal activity or other law enforcement-relevant event.

Below, we propose a hybrid solution for consideration that may square the circle between these competing policy considerations.

Always-On vs. Individual Control

In addition to whether or not law enforcement agencies should record audio as well as video from BWCs, the question arises as to whether or not the BWCs should record constantly throughout an officer's shift or if the officers should be able to start and stop the recordings at their discretion.

On the one hand, constant recording could unnecessarily invade the privacy of every individual with whom the officer comes into contact, including responding to a 911 call or other report of criminal activity, witnessing a crime and pursuing a suspect, serving a search or arrest warrant, or simply conducting day-to-day patrols and interacting with citizens on the street. Do we want all of our most intimate and embarrassing moments captured on police video and audio, with or without our advance consent?

More mundane, but equally important, if every officer in every department records every minute of every shift, the data generated will be staggering. In addition to the cost of storage, two potential consequences must be considered: Such volumes of data likely will compel many, if not most, agencies to utilize cloud storage of the BWC data, and searching, analyzing and retrieving such data, whether for prosecutions or misconduct investigations, will grow exponentially more difficult as the volume of data grows.

On the other hand, giving individual officers discretion to start and stop video and/or audio recordings generates another set of concerns.

One of the main perceived societal benefits of broad BWC deployment is deterring and documenting police misconduct, including racially-motivated violence and excessive use of force. Contrarily, a key benefit to police use of

BWCs is providing documentation to rebut false allegations of such violence or excessive force and to corroborate evidence of crimes being committed.

If officers can turn recordings on and off, the accuracy and thoroughness of such recordings will be called into question, including allegations, whether well-founded or not, that officers stopped recordings deliberately to cover up misconduct.

Also, anything short of constant recording will lead to excessive litigation, uncertainty and mistrust, negating much of the value of having BWCs in the first place.

Innovating to a Middle Ground

Although we are not engineers, we believe there may be a relatively simple technological innovation that could mitigate many of the risks raised above: BWCs could be set to record, at a minimum, video for the length of a police officer's shift, each equipped with a control switch. This switch would allow police officers to electronically tag the recording when the officer reasonably believes a law enforcement-relevant event is about to occur, as well as when an incident concludes.

Many, if not most, of these events likely will be preceded by a radio call, a police observation or some other triggering event, at which point an officer could touch the BWC control to tag the video. As a result, in the future, such portions of the recorded data could be located relatively easily for analysis, longer storage (than irrelevant law enforcement recordings) and retrieval.

Of course, law enforcement officers will not be 100 percent accurate in their tagging: some events expected to be law enforcement relevant will turn out not to be and vice versa. Nonetheless, such a system should substantially reduce allegations of, and litigation over, selective recording by police to cover up misconduct because there would be full recordings of each police officer's shift to resolve evidentiary disputes.

Except where related in time to a disputed incident, portions of video without such tags could be saved for relatively shorter periods of time since they will be more likely to contain embarrassing invasions of privacy or sensitive personal information without legal significance.

With such innovative technology, police could similarly toggle on and off audio recordings from BWCs, perhaps with policy requirements for gaining consent prior to activating the audio recording capabilities. Such a process also could enable supervisors to review, assess and modify officer training over time based on the accuracy and effects of tagging decisions made by individual officers.

Whether or not such technology is created and deployed, law enforcement officials and policymakers must rapidly agree on "best practices" for: the storage and security of BWC data; access to, analysis of and retention and destruction of data; analytics of the video and related metadata; issues of secondary use of BWC data (e.g., in criminal prosecutions unrelated to the incident for which a recording was initially made or civil lawsuits); and for how BWC-generated data should be handled under Freedom of Information Act (FOIA), sunshine law requests and records laws in the various states.

We will discuss these important issues, as well as vendor requirements and limitations for cloud storage providers, in our next article.

Bryan Cunningham is an information security, privacy, and data protection lawyer, and a senior advisor of The Chertoff Group (http://www.chertoffgroup.com/), a security and risk management advisory firm. Formerly, he was a U.S. civil servant, working for the CIA and serving as Deputy Legal Adviser to National Security Advisor Condoleezza Rice..

Nelson O. Bunn, Jr. is Director of Policy and Government Affairs at the National District Attorneys Association. He previously served as the Director of Government Affairs at The Charles Group, LLC, where he worked primarily with the Major County Sheriffs' Association, representing their views on numerous law enforcement issues.