With Body-Worn Cameras, Here Comes the Hard Part

Damian Dovarganes / AP File Photo

As law enforcement agencies implement these important policing tools, there are important issues with storing and protecting data and when to make it available to the public.

BY BRYAN CUNNINGHAM AND NELSON BUNN | NOVEMBER 23, 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 urged law enforcement agency (LEA) policymakers to address a broad and complex set of decisions that must be made sooner rather than later. We can now report good news and bad news. The good news is that at least five states—Arizona, Colorado, Illinois, Maryland and South Carolina—have either created study commissions to address some of these issues or passed legislation related to body-worn cameras.

The not-so-good news is that, at least based on publicly available information, while policymakers are wrestling with some of the BWC deployment and data collection issues we identified in our second piece

(http://www.nationaljournal.com/next-america/criminal-justice/which-data-should-police-body-cams-collect?mref=scroll), there does not appear to have been much deliberation on two sets of issues that we feel are both the most difficult and the most important with regards to BWCs.

In this final article, we take a deep dive into these issues vital for the long-term success of BWC deployment, both for law-enforcement officer protection and accountability and the safeguarding of the privacy and civil liberties of all of our citizens: first, the storage, analysis, protection and use of BWC-generated data; second, the susceptibility of such data to Freedom of Information, Sunshine Law and related requests for public disclosure of such data.

Storage, Analysis, Protection and Use of BWC Data

Given the massive volume, cost and complexity of handling BWC-generated data, many LEAs undoubtedly will opt for some sort of commercial cloud storage for such data. This is a potentially viable and attractive solution, *provided* that such data is stored, analyzed, protected, used and received pursuant to well-accepted and rigorous standards. One such standard, with which most U.S. LEAs already will be familiar, is the FBI Criminal Justice information System (CJIS) security policy. The International Association of Chiefs of Police (IACP) has published guidance (http://www.theiacp.org/portals/0/pdfs/GuidingPrinciplesonCloudComputingi consistent with the CJIS security standard, for LEA cloud storage of data. *LEA policymakers should seriously consider requiring compliance with applicable provisions of the IACP guidance for cloud storage of BWC data.*

Key requirements of this guidance include:

- Cloud storage and processing of all data at the **highest level of security** in order to be stored together. Highlighting the interest of hackers in BWCs and their data, at least one BWC solution sold to US LEAs already has been reported (http://news.softpedia.com/news/police-body-cameras-shipped-with-pre-installed-conficker-virus-496177.shtml) to come pre-loaded with a well-known type of malware. Applying a highest-common-denominator approach to BWCs and their data not only provides maximum protection for the integrity and privacy of the data captured by BWCs, but it also saves the time, personnel, resources and expense necessary to make individual determinations for each piece of data as to what level security should be applied.

- LEAs storing BWC data in the cloud should **prohibit cloud service providers from data mining** such information for any purpose not strictly related to the law-enforcement mission.

- **Protection of the confidentiality, availability, and integrity** of cloud-stored BWC data should be of paramount importance and required in all contracts with cloud storage providers. While such protection is cyber security 101, it is even more important in the context of LEA BWC data because of the certainty that a significant percentage of such data will have to be recovered and provided to criminal defendants and courts under strict chain-of-custody requirement. The IACP guidance suggests, among other protections: physical security measures, access permission requirements, cybersecurity requirements, criminal history background checks on employees and contractors with access to systems and data, and geographical location limitations.

- **Encryption Considerations.** End-to-end encryption of the BWC data would provide a high level of security for such data, which is an important consideration. However, unless such encrypted data can be thoroughly and accurately searched and recovered, and the chain-of-custody for criminal discovery purposes maintained, the use of such encryption could frustrate the constitutional rights of criminal defendants and create endless litigation for law-enforcement officers and the prosecutors who must represent the government in criminal proceedings. Without the ability to reliably search encrypted, cloud-stored data, LEAs likely would be forced to locally store duplicate copies of BWC-generated data, defeating the purpose of cloud storage and creating additional litigation. Of course, any cloud solution that does not include such encryption must employ alternative, but equally strong, security measures.

- **Decoupling of Storage and Analysis of Data With Collection Technology.** In some cases, the best and most cost-effective solution for LEA storage of BWC data may be to purchase storage analysis and use capabilities bundled with the cameras and other equipment that they purchase. This is not necessarily always the case, however, and LEA decision-makers should carefully consider “all-in” bundled solutions in which camera manufacturers offer storage and analysis solutions as well as hardware. Regardless of which solutions LEAs select, they should require storage providers to meet all of the criteria discussed in this article.

- **Analysis, Use and Repurposing of BWC Data.** LEA policy makers must decide early on the extent to which panel analysis and use maybe made of BWC-generated data for purposes other than individual criminal

prosecutions and investigations into allegations of LEA misconduct. For example, will analysis across different officers' records and cases be permitted for purposes of analyzing crime statistics and trends or determining the effectiveness of officer training? Likewise, decisions will have to be made about whether and how civil litigants in cases related to, e.g., child custody or insurance defense can request BWC data. Finally, and worthy of a separate discussion, is the issue of the public disclosure of such data pursuant to media, citizen, or public interest group requests.

Public Disclosure of BWC Data

As BWCs get closer to wide deployment in communities across the country, local law enforcement agencies and prosecutors are contemplating the necessity to balance the public and media's desire and, in some cases, right, to access footage of incidents that have occurred with the same public's expectations of privacy. According to the Reporters Committee for Freedom of the Press (http://www.rcfp.org/bodycams), 10 states have already passed legislation this year related to accessing footage created by body-worn cameras.

States have taken different approaches to when, if ever, BWC footage will be disclosed to the public. For example, South Carolina, the first state to pass comprehensive BWC legislation, prohibits BWC footage from being subject to the state's Freedom of Information Act (FOIA). Other states have limited who can access such footage by passing broad exemptions for law enforcement. Still others, like Washington State, have completely open records laws that allow all BWC footage to be accessed by the public, with agencies like the Seattle Police Department even uploading the footage to YouTube, albeit redacted.

One major obstacle to open public access to all BWC data is expense and personnel commitment required to review and redact the massive amount of such data (estimates are about two hours to redact for every one hour of footage) prior to public disclosure. Under the Seattle model, anyone can search through footage, looking for particular incidents of interest, file for more complete versions of the footage, and then receive such information. While this may expedite the process somewhat, the number of personnel hours that must go into redaction and editing of footage is enormous, coming at a high financial cost to any given agency.

Moreover, this approach puts the privacy of individuals, including innocent ones, caught on camera, in greater jeopardy. In a previous installment, we discussed sensitive situations likely to be subject to police BWC capture. These include incidents involving sexual assault, domestic violence, and those involving juveniles. Others might include embarrassing situations, or discussions of particularly sensitive personal information, to name a few. Most would agree that such private moments should not be routinely made available to the public. LEAs in jurisdictions allowing public access to BWC footage must create robust policies governing the public disclosure of BWC data.

Such policies also should address potential unintended consequences of broad public availability of BWC data. Does publicly available footage taint a jury pool and damage one's constitutional right to a fair and speedy trial? Does the footage allow for routine, lawful, and appropriate actions by law enforcement officers to get overly scrutinized by the public? Experts disagree about whether law enforcement has become more tepid in performing its duties due to the growing trend of footage being captured on cell phones and other handheld devices. Could officer safety be compromised?

Throughout our three-part series we have attempted to at least identify key issues that LEAs, and the policymakers that supervise them, must address now at the beginning of the BWC era. There are, of course, many additional and more detailed issues to be addressed, but we have attempted to highlight the most important, and most pressing ones. Though wide deployment by law enforcement agencies of BWCs is not a silver bullet, and does come with risks and tradeoffs, we hope this series will be broadly read across LEAs and will stimulate the development of appropriate policies so that BWCs can be used effectively to become a net win for justice.

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.