epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Statement for the Record of the

Electronic Privacy Information Center

Public Hearing on "Docket #0279, ordinance mandating use of body cameras by Boston Police and establishing proper procedures for usage "

Before the

Committee on Government Operations
Boston City Council

August 5, 2015
Boston City Hall
Boston, MA

Chairman Flaherty, Vice Chairman Jackson, and members of the Government Operations Committee of the Boston City Council, thank you for holding this hearing today. The hearing addresses a very timely and important issue—police body cameras.

The Electronic Privacy Information Center ("EPIC") is a non-partisan research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] We work with a distinguished panel of advisors in the fields of law, technology, and public policy.[2] EPIC is focused on the protection of individual privacy rights, and we are particularly interested in the privacy problems associated with video surveillance.[3] Police body cameras are a form of video surveillance, and like CCTVs, body cameras raise a number of privacy issues.

Body cameras do not simply record police activities; they record the activities of the public at large. They implicate the rights of innocent bystanders recorded on tape, particularly peaceful public protesters exercising their First Amendment rights. These devices could easily become a system of mass surveillance. Further, the benefits of body cameras as a tool of police accountability have not been established.[4] The study done of the police department in Rialto, California is often cited as proof that body cameras work, but as one of the researchers who conducted the study has said, "The Rialto study is one study. And it could be a fluke."[5] Among the questions that the Rialto study raised: Did the cameras make the differences or was it the awareness that officers would be subject to greater scrutiny? Are the effects maintained over time or are they likely to diminish?

Any deployment of body cameras must be accompanied by new policies and procedures and independent oversight to protect citizens' rights. And any law enforcement agency that uses body cameras must be prepared to comply with all current laws, including any open government laws.

To be clear, given the threat that police body cameras pose as a tool of general surveillance and the alternative methods available to achieve police accountability, EPIC opposes the deployment of body cameras. This is an intrusive and ineffective technology that does not address underlying problems with police accountability.

---

[1] *About EPIC*, EPIC, https://epic.org/epic/about.html.
[2] *EPIC Advisory Board*, EPIC, https://epic.org/epic/advisory_board.html.
[3] EPIC, *Video Surveillance* (2015), https://epic.org/privacy/surveillance/; *Comments of EPIC to DHS*, Docket No. DHS-2007-0076 CCTV: Developing Privacy Best Practices (2008), *available at* https://epic.org/privacy/surveillance/epic_cctv_011508.pdf; *Comments of EPIC to Metropolitan Police Department for the District of Columbia*, 53 D.C. Reg. 4462: Expansion of CCTV Pilot Program (2006), *available at* https://www.epic.org/privacy/surveillance/cctvcom062906.pdf; EPIC, *Spotlight on Surveillance: D.C.'s Camera System Should Focus on Emergencies, Not Daily Life* (2005), https://epic.org/privacy/surveillance/spotlight/1205/.
[4] *See* Michael D. White, *Police Body-Worn Cameras: Assessing the Evidence* (2014) (Suggesting there is a lack of research to support claims that body cameras are an effective police accountability measure).
[5] Martin Kaste, *Police Departments Issuing Body Cameras Discover Drawbacks*, NPR (Jan. 22, 2015), http://www.npr.org/sections/alltechconsidered/2015/01/22/379095338/how-police-body-camera-videos-are-perceived-can-be-complicated.

As a tool of general surveillance, police body cameras pose a significant threat to privacy and civil liberties. Furthermore, the full privacy risks that body cameras pose have not been assessed. Body cameras do not directly record police officers but are worn to point outwards as if from the view of the officer, thus focusing its surveillance on members of public. These cameras will often record people at their weakest, most embarrassing, or most personally sensitive moments. The body cameras will capture, for example, victims of domestic or sexual abuse after they have been attacked. They will record individuals that are inebriated, naked, or severely maimed or dead.

Many of these images are likely to end up on the Internet. In one particularly horrific example, the images of a young California girl who died tragically in a car accident were posted online by the California Highway Patrol. She was decapitated. The family sued the agency for the emotional harm that resulted. The agency settled with the family for 2.37 million dollars.[6] More recently, the Minneapolis Police Department released body camera footage that included the image of a woman's dead body.[7] The mother of the deceased woman was admitted to the hospital for chest pains after learning that the video had been released, and she is currently contemplating legal action.[8]

Body cameras have the potential to record a significant amount of footage of citizens not directly interacting with the police or implicated in any crime. Cameras on police will routinely record all of the surroundings, not simply interactions with possible criminals. That means that police will routinely record the images of all people they pass on the sidewalk or street. It means also that the police will record all images of people in a crowd. Much of this information will then become available to supervisors, vendors and others for review and evaluation. A program to promote police accountability could easily become the basis for mass surveillance of the general public.

Mass video surveillance undermines our expectation of privacy in public by permanently recording every detail of our actions. Individual public actions are barely noticed, but mass video surveillance creates a lasting record for infinite replay and scrutiny. The result is the chilling of our legal, constitutionally protected First Amendment activities.

There is also the possibility that body cameras could be coupled with facial recognition technology that will make it possible to identify people in public spaces even if they are not engaged in any suspicious activity. In Dubai, for example, the police will soon test Google Glass connected to a database of facial images.[9] The government says that it will help officers identify wanted criminals, but there is no reason the devices

---

[6] Dan Whitcomb, *California Family Settles Lawsuit Over Leaked Crash Images*, Reuters (Jan. 31. 2012), http://www.reuters.com/article/2012/02/01/us-crash-photos-settlement-idUSTRE81006220120201.
[7] Curtis Gilbert, *Police Body Cameras Reveal Minnesota Life Laid Bare*, MPR News (May 11, 2015), http://www.mprnews.org/story/2015/05/11/body-camera-footage.
[8] *Id.*
[9] Lily Hay Newman, *Dubai Police Will Wear Google Glass With Facial Recognition Software to ID Crooks*, Slate (Oct. 3, 2014), http://www.slate.com/blogs/future_tense/2014/10/03/dubai_police_will_use_facial_recognition_and_google_glass_to_look_for_wanted.html.

would not eventually be linked to general database of facial images. Similarly, the police in Britain are using facial recognition technology for both police body cameras and the six million CCTV cameras in the country.[10]

Long retention periods could exacerbate the use of facial recognition technology. Lengthy retention periods could allow for the tracking of a person's previous whereabouts through the use of facial recognition on the database of body camera recordings.[11] A similar database structure could develop like the one used for license plate readers where private companies manage billions of records that allow for the commercial data mining of data that goes back years.[12]

Current laws do not provide adequate protection against the identification of innocent individuals without their consent.[13] Consequently, the use of facial recognition technology by law enforcement agencies is expanding within the United States without proper oversight or input from the public. In 2013, the Chicago Police Department deployed facial recognition technology to use on images from surveillance cameras and other sources.[14] Similarly, the Seattle Police Department implemented facial recognition technology on the agency's repository of booking photos.[15]

As facial recognition technology moves forward, law enforcement at all levels will seek additional repositories of images to use the technology on. The FBI already uses facial recognition to compare subjects in FBI investigations to millions of license and identification photos retained by state DMVs.[16] The original purpose of ID and driver license photos was not law enforcement facial recognition searches. Over time, the use cases expanded.

History suggests that body camera recordings collected for the purpose of police accountability will eventually be used for secondary purposes beyond the original intent for its collection. Indeed, the Colorado police agencies are already considering adding

---

[10] Olivia Solon, *UK Police Hope to Catch Suspects with Facial Recognition Tech*, Wired UK (July 17, 2014), http://www.wired.co.uk/news/archive/2014-07/17/neoface.

[11] *See* Alexandra Mateescu, Alex Rosenblat, and danah boyd, *Police Body-Worn Cameras* (Data & Society Research Institute Working Paper 2015), *available at* http://www.datasociety.net/pubs/dcr/PoliceBodyWornCameras.pdf.

[12] *See id.*

[13] *See* Kyle Chayka, *The Facial Recognition Databases Are Coming. Why Aren't the Privacy Laws?*, The Guardian (Apr. 30, 2014), http://www.theguardian.com/commentisfree/2014/apr/30/facial-recognition-databases-privacy-laws.

[14] Chicago Police Department, *Department Notice D13-11: Facial Recognition Technology* (Aug. 23, 2013), http://directives.chicagopolice.org/directives/data/a7a57b38-140a7462-10914-0a74-6497bf3eec2deb9c.html?ownapi=1.

[15] Seattle Police Department, *12.045 – Booking Photo Comparison Software* (Mar. 19, 2014), http://www.seattle.gov/police-manual/title-12---department-information-systems/12045---booking-photo-comparison-software.

[16] Craig Timberg and Ellen Nakashima, *State Photo-ID Databases Become Troves for Police*, Washington Post (June 16, 2013), http://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html; *See also* EPIC, *FBI Performs Masive Virtual Line-up by Searching DMV Photos* (June 17, 2013), https://epic.org/2013/06/fbi-performs-massive-virtual-l.html.

facial recognition technology to body cameras.[17] As technology researchers danah boyd and Alex Rosenblat point out, "new surveillance and data-collection practices in law enforcement have already created frames for broadening police powers, and in particular, for increasing the over-policing of communities of color."[18] Body cameras threaten to become the next surveillance technology disproportionately aimed at the most marginalized members of society.

The rise in the push for the implementation of police body-worn cameras comes from a general push for better police accountability. It's fair to say that law enforcement has an institutional problem with accountability. It's not just about a few bad actors but about an institution and a culture that often protects these bad actors from consequences. Technology, specifically body cameras, is not the answer to this problem.[19] More surveillance is never the solution but a crutch for bad, ineffective, or improperly implemented policies. There are other, more productive means to achieve accountability that do not carry the risk of increasing surveillance and undermining privacy and civil liberties.

Better transparency, accountability, and oversight need to be instilled into police departments. Accountability needs to be part of police culture at all levels and for all tasks that have a bearing on how well officers perform their duties to serve and protect. Instead of Boston spending millions of dollars on new technology, the city should focus on correcting current policies and procedures associated with hiring, training, and discipline—among other areas—to maximize accountability of individual police officers and the department.

As stated at the beginning, EPIC is against the deployment of body cameras. But, if the Boston Police deploy body cameras, EPIC recommends the following measures:

⇒ **No Exemption from open government laws**
- *Open Government Laws Must be Adhered to*: Open government laws are an important tool for public accountability and body cameras, as a police accountability measure, should not be exempt from open government laws. If the obligations of open government laws cannot be met, including obligations to protect personal privacy, the law enforcement agency should not deploy body cameras.

⇒ **Limit Collection**
- *Body Camera Footage That Does Not Involve Active Police Work Should Not Be Retained*: Only footage associated with police interactions with the public or crime scenes should be retained. Footage of, for example, the officer merely walking down a busy street should not be recorded.

---

[17] Michael De Yoanna, *Colorado Police Cautiously Eager About Body Cameras That Recognize Faces*, Colorado Public Radio (July 19, 2015), http://www.cpr.org/news/story/colorado-police-cautiously-eager-about-body-cameras-recognize-faces.
[18] danah boyd and Alex Rosenblat, *It's Not Too Late to Get Body Cameras Right*, The Atlantic (May 15, 2015), http://www.theatlantic.com/technology/archive/2015/05/its-not-too-late-to-get-body-cameras-right/393257/.
[19] *See id.*

⇒ **Limit Use**
- *Body Cameras Should be Used for Police Accountability Only*: The use of body camera recordings should not be expanded beyond uses associated with police accountability now or in the future. The use of body cameras for any form of surveillance should be strictly banned.

⇒ **Limit Access**
- *Access to Body Camera Recordings Should be Limited*: Access to footage should be limited to reasons related to police accountability. Law enforcement agencies should maintain an audit trail of who accesses the footage and for what reason.

⇒ **Adequate Security**
- *Body Camera Recordings Should be Kept in a Secure Manner to Prevent Theft, Leaks, or Improper Access*.

⇒ **Limit Retention**
- *Body Camera Recordings Should Only be Kept Long Enough to Serve the Purpose of Police Accountability*: Retention of body camera data should be counted in days or weeks—not months or years. Data should be deleted on a periodic basis unless necessary to ensure police accountability.

Our preference would be that police body cameras be used solely for training exercises to assist officers working with supervisors to develop appropriate skills to ensure that procedures are followed during interactions with the public. In this context, it is possible to view body cameras as useful tools for police training. But once these cameras are used in a public setting and capture the images of actual people, many who will be in distress, the privacy concerns will skyrocket and the risks of litigation against the city will become very real.

Conclusion

It is imperative that police departments across the country proactively confront police abuse with accountability, oversight, and transparency measures that create a culture of accountability.[20] Body cameras will not do this. Better policies will.

[20] See Appendix A for alternative suggestions to body cameras for police accountability.

Appendix A

Alternative Suggestions to Body Cameras for Police Accountability

⇒ **Hiring**
- *Assessing Candidates for the Job*: Hiring should include an assessment of a candidates potential for abuse including whether the candidate has the skills to address tough situations without unnecessarily escalating the situation.
- *Holding Hiring Officers Accountable*: Those who hire police officers should be held accountable for hiring abusive officers who had red flags during the hiring process or for not implementing tailored training programs to address any red flags as part of the hiring process.

⇒ **Training**
- *Proper training*: Officers should receive training in how to properly interact with all individuals in order to maximize the chances that situations do not escalate.

⇒ **Identifying and Disciplining Abusive Officers**
- *Taking First-time and Minor Abuses Seriously*: Initial and minor abuses need to be taken seriously as indicators of a potentially larger problem. Appropriate training or re-training should be required and the seriousness of even minor abuses should be conveyed.
- *Disciplining Officers*: Discipline for abusive officers should be strong enough to act as a deterrent and convey the seriousness of the issue. The police department should not tolerate officers who show a pattern of abuse and supervising officers should be held accountable for repeat offenders they failed to properly discipline.
- *Disciplining Complicit Officers*: Officers who fail to report abuse should be disciplined.

⇒ **Independent Oversight**
- *Implement Independent Oversight*: Independent oversight is required to ensure compliance with the implemented measures of accountability.

⇒ **Transparency**
- *Public transparency*: Public transparency measures are necessary including a periodic report detailing the number of police officer abuse incidents, the type of incidents, and the discipline meted out.