epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

November 4, 2019

Council Member Charles Allen, Chairperson
Council for the District of Columbia
Committee on the Judiciary & Public Safety
1350 Pennsylvania Ave. NW
Washington, DC 20004

RE: Public Oversight Roundtable on Five Years of the Metropolitan Police Department's Body-Worn Camera Program: Reflections and Next Steps

Dear Chairman Allen and Members of the Committee on the Judiciary & Public Safety:

We write to you about the hearing on the Police Department's Body-Worn Camera Program to remind the Committee of EPIC's previous testimony before the Committee and to highlight growing support for a moratorium on the use of face recognition technology. EPIC previously testified before the DC City Council in 2008, warning that "facial recognition will make it possible to identify people in public places."[1]

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.[2] EPIC is focused on the protection of individual privacy rights, and we are particularly interested in the privacy problems associated with video surveillance in Washington, DC. Police body-worn cameras are a form of video surveillance, and like CCTVs, body-worn cameras raise a number of privacy issues.

EPIC launched a campaign in 2002 to draw attention to public concerns about the use of video surveillance in the nation's capital. EPIC highlighted the history of public protest in Washington, DC and warned the camera surveillance threatened to chill protected First Amendment activity.[3]

In 2015, EPIC testified before the D.C. City Council, arguing that police body cameras were "an intrusive and ineffective technology that does not address underlying problems with police accountability."[4] In 2017, a study to assess the benefits of the body cameras worn by the

---

[1] *Video Interoperability for Public Safety: Hearing Before Comm. on Public Safety and the Judiciary of the D.C. Council* (June 2, 2008) (statement of Marc Rotenberg, Executive Director, EPIC), *available at* https://epic.org/privacy/surveillance/dccouncil_cctv060208.pdf.
[2] *About EPIC*, EPIC, https://epic.org/epic/about.html.
[3] *Observing Surveillance*, http://observingsurveillance.org.
[4] *Public Oversight Roundtable on the Metropolitan Police Department's Body-Worn Camera Program: Hearing Before the Comm. on the Judiciary of the D.C. Council* (May 7, 2015) (statement of Jeramie D. Scott, National Security Counsel, EPIC), *available at* https://epic.org/privacy/testimony/EPIC-DC-Council-Body-Camera-Testimony.pdf.

Metropolitan Police Department concluded that the cameras had no impact on police use of force and civilian complaints.[5]

EPIC attaches our previous statement to remind the Committee of the 1) privacy issues associated with body-worn cameras, 2) need for transparency and adherence to the obligations of the Freedom of Information Act, and 3) alternatives to body-worn cameras to address police accountability.

One of the most critical privacy issues currently associated with video surveillance is the use of face recognition technology. Facial recognition poses threats to privacy and civil liberties. Facial recognition techniques can be deployed covertly, remotely, and on a mass scale. There is a lack of well-defined regulations controlling the collection, use, dissemination, and retention of biometric identifiers. Ubiquitous identification by government agencies eliminates the individual's ability to control the disclosure of their identities, creates new opportunities for tracking and monitoring, and poses a specific risk to the First Amendment rights of free association and free expression.[6]

Consequently, there has been growing opposition to the deployment of facial recognition technology. There is a national effort in the U.S. to ban the use of facial recognition by the government.[7] California has already enacted a law banning the use of facial recognition technology in law enforcement body cameras.[8] Additionally, San Francisco, Berkeley, and Oakland, California and Somerville, Mass. have all passed local bans on the use of facial recognition by city agencies.[9]

At the annual international meeting of the privacy commissioners, EPIC presented a declaration from more than 90 civil society organizations and several hundred experts calling for a moratorium on the further deployment of facial recognition.[10] The civil society organizations and experts urged countries to:

1. suspend the further deployment of facial recognition technology for mass surveillance;
2. review all facial recognition systems to determine whether personal data was obtained lawfully and to destroy data that was obtained unlawfully;
3. undertake research to assess bias, privacy and data protection, risk, and cyber vulnerability, as well as the ethical, legal, and social implications associated with the deployment of facial recognition technologies; and
4. establish the legal rules, technical standards, and ethical guidelines necessary to safeguard fundamental rights and comply with legal obligations before further deployment of this technology occurs.

---

[5] David Yokum *et al.*, *Evaluating the Effects of Police Body-Worn Cameras: A Randomized Controlled Trial* (Oct. 20, 2017), http://bwc.thelab.dc.gov/TheLabDC_MPD_BWC_Working_Paper_10.20.17.pdf.
[6] *See* Ian Kerr & Jennifer Barrigar, *Privacy, Identity and Anonymity* (Apr. 1, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3396076.
[7] Ban Facial Recognition, https://www.banfacialrecognition.com.
[8] 2019 Cal. Legis. Serv. Ch. 579 (A.B. 1215).
[9] *See* EPIC, State Facial Recognition Policy, https://epic.org/state-policy/facialrecognition/.
[10] Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance Endorsements, https://thepublicvoice.org/ban-facial-recognition/.

The use of facial recognition technology on police body-cameras would turn a tool of police accountability into a mobile-mass surveillance platform.[11] EPIC urges the D.C. City Council to proactively prevent this from happening and ban the use of facial recognition technology on police body-worn cameras.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Jeramie Scott*
Jeramie Scott
EPIC Senior Counsel

Encl.

[11] Jeramie D. Scott, *Police Body Cameras: Accountability or Public Surveillance?* (Jan. 29, 2015), https://blog.epic.org/2015/01/29/police-body-cameras-accountability-or-public-surveillance/.

Statement for the Record of

Jeramie D. Scott
National Security Counsel
Electronic Privacy Information Center

Public Oversight Roundtable on the Metropolitan Police Department's Body-Worn Camera Program

Hearing before the

Committee on the Judiciary

Council of the District of Columbia

May 7, 2015
Washington, D.C.

Chairman McDuffie and members of the Committee on the Judiciary, thank you for holding this public hearing today. The hearing addresses a very timely and important issue—police body-worn cameras.

My name is Jeramie Scott, and I am the National Security Counsel for the Electronic Privacy Information Center or simply EPIC. 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-worn cameras are a form of video surveillance, and like CCTVs, body-worn cameras raise a number of privacy issues.

EPIC previously testified before the D.C. Council on the Council's efforts to create a legal framework for the use of video surveillance in Washington, DC.[4] In that testimony, EPIC stated that video surveillance raises Constitutional issues; the benefits of video surveillance are overstated; and that any implementation of video surveillance needed strong policy and procedures and independent oversight to protect citizen's rights.[5] The DC City Council adopted several of EPIC's proposals, including restrictions on the collection and use of personal information.[6]

Police body worn cameras raise similar 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 who frequently gather in the Nation's capital. 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.[7]

If the DC City Council and the Metropolitan Police Department ("MPD") go forward with the deployment of body cameras, there must be new policy and procedures

---

[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] *Joint Public Oversight Hearing: Comm. on the Jud. On Public Works and the Environment City Council of the District of Columbia* (2002) (Statement of Marc Rotenberg, EPIC Executive Director), available at https://epic.org/privacy/surveillance/testimony_061302.html.
[5] *Id.*
[6] *See* 24 DCMR §§ 2500-2599.
[7] *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).

and independent oversight established to protect citizens' rights. And the MPD must be prepared to comply with all current laws, including the Freedom of Information Act.[8]

But let me be clear, given the threat that police body-worn 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.

As a tool of general surveillance, police worn-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.[9]

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

[8] DC Code §§ 2-531 – 539.
[9] 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.

soon test Google Glass, connected to a database of facial images.[10] The government says that it will help officers identify wanted criminals, but there is no reason the devices 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.[11]

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.[12] 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.[13]

Current laws do not provide adequate protection against the identification of innocent individuals without their consent.[14] 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.[15] Similarly, the Seattle Police Department implemented facial recognition technology on the agency's repository of booking photos.[16]

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.[17] The original purpose of ID and driver license photos was not facial recognition searches. Over time, the use cases expanded.

---

[10] 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.

[11] 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.

[12] *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.

[13] *See id.*

[14] *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.

[15] 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.

[16] 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.

[17] 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*

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.

The rise in the push for the implementation of police body-worn cameras comes from a general push for better police accountability. I think 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. 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. The MPD could lead the way as an example of how to hold police accountable without threatening 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 spending millions of dollars on new technology, the MPD should focus on correcting current policies and procedures associated with hiring, training, and discipline—among other areas—to maximize police accountability individually and as a department.

As I stated at the beginning, EPIC is against the MPD's deployment of body cameras. But, if the MPD insists on implementing body-worn cameras, EPIC recommends the following measures:

⇒ **No Exemption from FOIA**
- *Freedom of Information Act Obligations Must be Met*: FOIA is an important tool for public accountability and body cameras, as a police accountability measure, should not be exempt from FOIA. If FOIA obligations cannot be met, including obligations to protect personal privacy, MPD 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.

⇒ **Limit Use**
- *Body Cameras Should be Used for Police Accountability Only*: The use of body camera recording should not be expanded beyond uses associated

---

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.

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. The MPD 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 the MPD, and other police departments across the country, proactively confront police abuse with accountability, oversight, and transparency measures that create a culture of accountability.[18] Body cameras will not do this. Better policies will.

[18] See Appendix A for a few alternative police accountability recommendations to body cameras.

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 Compliant 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.