

1634 I Street, NW Suite 1100 Washington, DC 20006

> P +1-202-637-9800 F +1-202-637-0968 E info@cdt.org

> > January 28, 2015

President's Task Force on 21st Century Policing Office of Community Oriented Policing Services U.S. Department of Justice 145 N Street, N.E. 11th Floor Washington, DC 20530 comment@taskforcepolicing.us

Dear Members of the Task Force on 21st Century Policing:

The Center for Democracy & Technology (CDT) writes to provide recommendations related to body-worn cameras in response to the Task Force's consideration of the issue and request for public comment. CDT is a nonpartisan, non-profit technology policy advocacy organization dedicated to protecting civil liberties and human rights while encouraging the continued development of the Internet and other technological innovations that empower individuals. With use of body cameras rapidly expanding across the country and federal legislation being offered for nationwide use, we are pleased to see the Task Force addressing this important new technology, and its impact on privacy and civil liberties.

Body cameras have significant promise to reduce misconduct and increase public confidence in law enforcement.⁴ However, they also represent a powerful new technology that could be co-opted as tool for

¹ COPS Office, *Listening Session: Technology and Social Media*, available at http://www.cops.usdoj.gov/Default.asp?ltem=2768.

² See generally, Michael D. White, *Police Officer Body-Worn Cameras: Assessing the Evidence*, Office of Community Oriented Policing Services, *available at* https://ojpdiagnosticcenter.org/sites/default/files/spotlight/download/Police%20Officer%20Body-Worn%20Cameras.pdf, *hereafter*, *Assessing the Evidence Body Camera Study*.

³ See e.g., the Camera Authorization and Maintenance Act, which would require all state and local law enforcement agencies that receive Department of Justice grants to have their officers wear body cameras. H.R. 5865, 2014.

⁴ In one pilot program study, use of body cameras reduced citizen complaints against the police by 88 percent and decreased police use of force by 60 percent. *Assessing the Evidence Body Camera Study* at 20.

mass surveillance. While initial use of body cameras has been encouraging, varying standards threaten to cause serious privacy harms. We believe the Task Force should put forward recommendations for use of body cameras to serve as guiding principles for programs being implemented throughout the country, as well as for any federal legislation expanding the role of body cameras or requiring their use. Federal funding for camera use should be tied to both best practices and robust involvement from local communities controlling how camera technology is deployed and used.

Recommendations for use of body cameras⁵ must address the following areas:

1) Requirements and Limits for Recording: The most fundamental policy question is when cameras should be on. This policy should strive to make sure any potential interaction that could result in misconduct or a complaint is recorded, but also account for privacy interests of both officers and civilians, and questions of practicality. Research demonstrates that providing greater discretion for when cameras must be turned on results in a substantial decrease in video recordings.6 Therefore, a model general recording requirement should limit discretion, and require cameras generally be turned on whenever officers are interacting with the public. The Police Executive Research Forum also recommends a broad recording policy. However, a broad general recording policy should be paired with strong exceptions to compensate for privacy needs of both officers and civilians. An effective means of addressing this may be to require that cameras be turned off in locations where civilians have a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms.8 However, a more strict recording policy may be necessary when responding to a call for service or engaging in a law enforcement activity to guarantee oversight of the most critical interactions between the police and public. Finally, policies should ensure that issues of practicality do not interfere with general recording requirements, such as requirements that cameras are equipped with a "pre-event video buffer" and standardized rules for switching batteries and maintenance checks of cameras.

⁹ TASER International's AXON system, a commonly used body camera system, includes a battery pack that generally lasts 12 to 14 hours. See, *PERF Recommendations Report* at 10.



⁵ While our recommendations discuss body cameras, similar guidelines should exist for other oversight technologies such as cameras mounted on firearms and Tasers.

⁶ A yearlong test study in Mesa resulted in a 42 percent decrease in body camera use when a more discretionary policy was in effect For a six months period, the Mesa police department employed a policy that, "When practical, officers will make every effort to activate the on-officer body camera when responding to a call or have any contact with the public." For the following six months, the policy was changed to have officers "exercise discretion and activate the on-officer body camera when they deem it appropriate." Officers recorded 42 percent less video files during the second six-month period when the discretionary policy was in effect. Assessing the Evidence Body Camera Study at 8-9.

⁷ Miller, Lindsay, Jessica Toliver, and Police Executive Research Forum, *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned.* Washington, DC: Office of Community Oriented Policing Services (2014), 40, *available at* http://www.justice.gov/iso/opa/resources/472014912134715246869.pdf, hereafter, PERF Recommendations Report.

⁸ This restriction already exists in some jurisdictions using body cameras such as Salt Lake City. See, Utah police regulations III-535 MOBILE VIDEO RECORDERS.

Further, because federal wiretap laws and state peeping tom laws in many states prohibit video recording in such situations, the bounds of a "reasonable expectation of privacy" standard have strong legal foundation and can be readily adopted for body cameras.

- 2) Rules for Notification and Opting-Out: While a broad recording policy is advisable to ensure that important interactions and potential misconduct are recorded, 10 individuals should be given as much control as possible in regulating what video directed at them, and the ability to "opt out" as desired. This will promote individual privacy from unwanted government surveillance, but also facilitate police interviews with witnesses that may be reluctant to discuss an investigation on video. Generally, requiring officers to turn off a body camera when requested by an individual being recorded is consistent with existing body camera guidelines in numerous jurisdiction where state law requires consent to record. 11 Additionally, allowing for individuals to opt out will better ensure that crime victims and witnesses will not refuse to interact with officers out of fear of being recorded as cooperating, a significant concern for police departments. 12 In order to achieve this goal, some form of notification should be required that cameras are recording. This could occur via an explicit statement – as is required by departments in jurisdictions with two-party consent laws¹³ – or through indirect notification such as a "recording" light accompanying a camera. Quite simply, individuals cannot exercise a right to opt out of being recorded if they do not know a video feed is on.
- 3) Requirements and Limits on Retention: Limitations on retention are a crucial after the fact method of ensuring that body cameras serve as an oversight tool, and prevent creeping use of cameras for dragnet surveillance. However, limits on retention must account for factors such as civilian complaints, evidentiary use, and examination of evidence by criminal defendants. As an overall baseline, departments should be required to retain all video for the length of time civilians may file complaints. 14 Evidentiary video - video consisting of "an incident or encounter that could prove useful for investigative purposes, such as a crime, an arrest or citation, a search, a use of force incident, or a confrontational encounter with a member of the public,"¹⁵ – has significant potential value for civilian complains of misconduct, criminal investigations, and criminal defendants. However, the range of criminal offenses should be taken into account in establishing longer retention periods for evidentiary video; the value of video related minor and non-violent crimes must be weighted against technical limits to storage and privacy concerns. State evidentiary rules could serve as an effective foundation for obtaining this balance, where evidence for minor crimes is limited, but evidence for more serious crimes such as homicides – can be indefinite. 16 At a minimum, evidentiary video should be retained until adjudication or final disposition of the relevant investigation, to permit

¹⁰ See, PERF Recommendations Report at 12-14.

¹¹ See, Assessing the Evidence Body Camera Study at 27; see also, PERF Recommendations Report at 14.

¹² *Id*, at 12 ("[O]fficer discretion is needed in sensitive situations, such as encounters with crime victims or witnesses who are concerned about retaliation if they are seen as cooperating with the police"); *see also*, *Assessing the Evidence Body Camera Study* at 27.

¹³ PERF Recommendations Report at 56.

¹⁴ This is the leading factor for retention policy in a number of jurisdictions employing body cameras. *Id* at 17.

¹⁶ See, Id at 16 ("For example, many state laws require that footage involving a homicide be retained indefinitely, but video of a traffic citation must be kept for only a matter of months").

review by potential criminal defendants.¹⁷ However, beyond these fairly narrow circumstance – evidence of a crime or police misconduct – video footage should be promptly deleted.

While video is being retained, access should be limited. Video should be generally inaccessible, unless needed as evidence or for internal investigations. Strict prohibitions should exist against any editing of video apart from the retention rules for scheduled deletion. Officers should not have access to their own feed prior to filing of reports to prevent retroactive development of justifications for police actions, such as a Terry stop or arrest. High standards for data security should exist, regardless of whether videos are directly held by the department or a third party storage provider.¹⁸

4) Limits and Protections Regarding Dissemination: While the added accountability of body cameras can only be achieved if video feed can be released to affected civilians and other parties devoted to oversight, dissemination rules must account for the privacy interests of those being recorded, especially given that such recordings can occur in intimate situations such as the execution of a search warrant or interviewing of a crime victim. Furthermore, dissemination rules should account for issues of practicality. While civilians alleging police misconduct will have the most direct interest in obtaining video from body cameras, other parties – such as civil rights groups, government transparency groups, and media – will also have a legitimate interest in obtaining video feed for legitimate goals related to enhancing accountability and supporting the public interest.

However, if body camera video feed is to be made generally available, precautions should exist to protect the privacy of individuals recorded, especially given potential sensitivity of police interactions. Therefore, body camera feeds should be redacted to block 1) any personally identifiable information and 2) video whose disclosure constitutes a clearly unwarranted invasion of personal privacy.²⁰ The Police Executive Research Forum supports a broad disclosure policy containing exemptions for sensitive private information.²¹ While redaction efforts will require time and resources, tools such as face blurring technology can make the process



¹⁷ However, maintaining ability to obtain video for civilian complaints should always be the dispositive rule. If this is shorter than the length of time civilians may file misconduct complaints, retention should be extended to this time period.

¹⁸ PERF Recommendations Report at 44 ("[A]gencies should take all possible steps to protect the integrity and security of the data. This includes explicitly stating who has access to the data and under what circumstances, creating an audit system for monitoring access, ensuring there is a reliable back-up system, specifying how data will be downloaded from the camera, and including protections against data tampering prior to downloading").

¹⁹ In states such as Washington where video requests are governed by unrestricted public record laws, police departments have been overwhelmed with the magnitude of requests received. *See, Washington State police overwhelmed by public requests for dash- and body-cam footage*, Homeland Security News Wire (November 27, 2014), *available at* http://www.homelandsecuritynewswire.com/dr20141127-washington-state-police-overwhelmed-by-public-requests-for-dash-and-bodycam-footage.

²⁰ This requirement is adopted from the Utah public records request law – GRAMA – which governs the Salt Lake City Police Department's rules for dissemination of video from its body camera program. See, UCA 63G-2-302(2)(d).

²¹ See, PERF Recommendations Report at 17.

significantly easier, and are already being employed by some departments.²² Required redactions could be waived if the affected party consents to their release.

5) Limits on Use of Facial Recognition: Use of facial recognition in combination with body cameras represents a significant risk to privacy. In order to prevent overbroad surveillance and monitoring, use of facial recognition for recordings from police body cameras should be barred or sharply limited. Development of face prints from body cameras represents a significant threat to privacy, and activities protected by the First Amendment. Face prints could be cataloged from officers' recordings of religious ceremonies, political rallies, or public protests, such as developing a face print identification lists of all individuals in a Mosque or attending a "Black Lives Matter" demonstration.²³

Allowing officers to run *existing* face prints against video that is being recorded from body cameras offers risks to privacy as well. This practice could be used to locate, and monitor the activities of individuals not suspected of wrongdoing, especially in cities with large police forces.²⁴ Courts and state legislatures are increasingly recognizing the privacy value of location information – including in public – and establishing warrant-for-location requirements. Use of facial recognition in combination with body cameras should not serve as a loophole for these protections.

We are confident that body cameras can be a significant aid to safe and effective policing in the 21st century, and that with appropriate guidelines, their use will not inhibit privacy or civil liberties. We look forward to the chance to work with the Task Force in achieving these goals. If you have any questions regarding our comments, please contact Chris Calabrese, Senior Policy Director, at ccalabrese@cdt.org, or Jake Laperruque, Fellow on Privacy, Surveillance, and Security, at laperruque@cdt.org.

Sincerely,

Chris Calabrese Jake Laperruque

Senior Policy Director Fellow on Privacy, Surveillance, and Security

²² See e.g., Jon Fingas, Seattle police get help publishing body camera videos online, Engadget (November 24, 2014), available at http://www.engadget.com/2014/11/24/seattle-police-get-help-posting-body-camera-videos/.

²⁴ Chicago and Washington DC contain on average over 50 officers per square mile, while New York City contains an average of 119 officers per square mile. All three cities are currently implementing body camera programs. Whet Moser, *City Size and Police Presence*, Chicago Magazine (August 30, 2012), *available at* http://www.chicagomag.com/Chicago-Magazine/The-312/August-2012/City-Size-and-Police-Presence/.



²³ The NYPD "Demographic Unit" tasked with monitoring the activities of Muslim communities and FBI presentation highlighting potential use of facial recognition technology to tag individuals at campaign rallies reflect that these are genuine concerns *See*, Matt Appuzo and Joseph Goldstein, *New York Drops Unit That Spied on Muslims*, The New York Times (April 15, 2014), *available at* https://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html?r=0; *see also*, Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, Federal Bureau of Investigations, 4, *available at* https://www.eff.org/files/filenode/vorder-bruegge-facial-recognition-and-identification-initiatives-0.pdf