The Privacy Case for Body Cameras: The Need for a Privacy-Centric Approach to Body Camera Policymaking

ETHAN THOMAS*

Body-mounted cameras are being used by law enforcement with increasing frequency throughout the United States, with calls from government leaders and advocacy groups to further increase their integration with routine police practices. As the technology becomes more common in availability and use, however, concerns grow as to how more-frequent and more-personal video recording affects privacy interests, as well as how policies can both protect privacy and fulfill the promise of increased official oversight.

This Note advocates for a privacy-centric approach to body camera policymaking, positing that such a framework will best serve the public's multifaceted privacy interests without compromising the ability of body cameras to monitor law-enforcement misconduct. Part I surveys the existing technology and commonplace views of privacy and accountability. Part II examines the unique privacy risks imposed by the technology as well as the countervailing potential for privacy enhancement, demonstrating the value of an approach oriented around privacy interests. Part III assesses how the failure to adopt this approach has resulted in storage policies for body camera footage that inhibit the technology's ability to best serve the public and suggests that a privacy-centric perspective can lead to better policymaking. Finally, Part IV examines the flaws of prevailing views with respect to policies for accessing footage and discusses how a revised privacy-centric perspective could lead to better policies.

---

* Design & Layout Editor, Finance Editor, Colum. J.L. & Soc. Probs., 2016–2017. J.D. Candidate 2017, Columbia Law School. The author thanks David Pozen for his extensive help in developing this topic and the substance of this Note. The author also thanks the *Journal* editorial staff — especially Tara Raam, Nico Gurian, and Katie Aber — for their thorough assistance in editing and revision.

I. INTRODUCTION

Across the United States, governments, advocacy groups, and the general public have given significantly increased attention to body-mounted cameras for police officers in recent years as a means of documenting and deterring law-enforcement misconduct. Many of the most populous cities in the United States have already started to use body camera technology to some extent.[1] In late 2014, following unrest and controversy over police tactics in Ferguson, Missouri, President Obama called for increased funding and consistent policies for body camera programs across the nation, and the Department of Justice recently approved a major funding initiative to enable more departments to use the technology.[2] Following widespread protests after the 2015 release of a police dashboard camera video depicting a police shooting, Chicago committed to expanding its body camera program.[3] However, despite support for the technology and its potential to record and deter police misconduct, many have cited serious concerns about privacy. The prevailing narrative, in fact, seems to

---

1. *See* Zusha Elinson, *More Officers Wearing Body Cameras*, WALL ST. J. (Aug. 15, 2014), http://www.wsj.com/articles/body-cameras-on-police-can-reduce-use-of-force-citizen-complaints-1408134549 [https://perma.cc/PZ7G-DUEN] ("A 2013 study found that a quarter of 254 U.S. police departments surveyed used body cameras. . . . More than 1,200 law enforcement agencies have purchased wearable cameras from Taser International Inc., with about 80% of the company's camera sales occurring in the last 12 months . . . ."); Abigail Tracy & EJ Fox, *Is Your Police Force Wearing Body Cameras?*, VOCATIV (Nov. 15, 2014), http://www.vocativ.com/usa/justice-usa/police-force-wearing-body-cameras [https://perma.cc/XEJ4-73ZT] (2014 report finding that of the "100 most populous U.S. cities . . . 41 cities use body cams on some of their officers, 25 have plans to implement body cams and 30 cities do not use or plan to use cams at this time").

Some cities, however, have resisted the technology. *See* Jeff Goldstein, *Not One New York Police Officer Has a Body Camera*, N.Y. TIMES (Oct. 4, 2016), http://www.nytimes.com/2016/10/04/nyregion/despite-national-trend-new-york-police-are-slow-to-adopt-body-cameras.html [https://perma.cc/Q2EG-N6BR] ("[N]ot one of the [New York Police D]epartment's approximately 35,800 officers is wearing a body camera, even as the devices have become a staple for officers elsewhere.").

2. *See, e.g.*, Colleen McCain Nelson & Byron Tau, *Obama Calls for Policing Standards, Funding in Wake of Ferguson*, WALL ST. J. (Dec. 1, 2014), http://www.wsj.com/articles/obama-to-focus-on-ferguson-protests-in-monday-meetings-1417446423 [https://perma.cc/C6ED-6RYC]; Press Release, Dep't of Justice, Justice Department Awards over $23 Million in Funding for Body Worn Camera Pilot Program to Support Law Enforcement Agencies in 32 States (Sept. 21, 2015), https://www.justice.gov/opa/pr/justice-department-awards-over-23-million-funding-body-worn-camera-pilot-program-support-law [https://perma.cc/3WFN-B4HW].

3. *See* Monica Davey, *Chicago to Expand Use of Police Body Cameras*, N.Y. TIMES (Nov. 29, 2015), http://www.nytimes.com/2015/11/30/us/chicago-police-body-cameras.html [https://perma.cc/6KFA-3UXP].

frame privacy as the primary reason to resist the expansion of such programs.

The American Civil Liberties Union (ACLU) has been a notable advocate for body camera programs, as well as a leader in crafting policy recommendations, and its support demonstrates this privacy-security tension. The ACLU embraces the technology despite typically holding a "dim view of the proliferation of security cameras in American life,"[4] because the potential of such technology to serve as an effective check against abuses of law-enforcement power outweighs concerns of increased recording.[5] Nonetheless, the ACLU qualifies its endorsement with a caution that body camera implementation must be accompanied by the right policies, recognizing that "body cameras have more of a potential to invade privacy than" other camera systems used to ensure official accountability, such as dashboard and prison cameras.[6] The ACLU recommends several policies that it believes can result in a "win-win" by striking the right balance between privacy interests and police accountability issues,[7] thus protecting the public from police misconduct and protecting the police from false allegations of abuse.[8]

Organizations that have implemented body camera systems, however, have at times drawn criticism for failing to make policies that effectively curb abuse. For instance, the Los Angeles Police Department (LAPD) recently began implementing a plan to equip every officer with a body camera.[9] The policies required frequent recording and prohibited tampering with footage, but nonetheless lost the ACLU's support because the body camera policies lacked adequate checks against police officers abusing the

4. JAY STANLEY, ACLU, POLICE BODY-MOUNTED CAMERAS: WITH RIGHT POLICIES IN PLACE, A WIN FOR ALL 2 (2d ed. 2015), *available at* https://www.aclu.org/sites/default/files/assets/police_body-mounted_cameras-v2.pdf [https://perma.cc/D48R-BJXP] [hereinafter ACLU RECOMMENDATIONS].

5. *See id.* (recognizing the "potential to invade privacy," but nonetheless endorsing the technology because "when cameras primarily serve the function of allowing public monitoring of the government instead of the other way around, we generally support their use.").

6. *Id.*

7. *See id.* ("[T]he challenge of on-officer cameras is the tension between their potential to invade privacy and their strong benefit in promoting police accountability.").

8. *See id.*

9. Kate Mather, *Divided Police Commission Approves Rules for LAPD Body Cameras*, L.A. TIMES (Apr. 28, 2015), http://www.latimes.com/local/lanow/la-me-ln-lapd-body-cameras-rules-20150427-story.html [https://perma.cc/PWL7-GMP3].

footage.[10] A particularly controversial provision of the LAPD policy required officers to review footage of an incident before preparing a report.[11] One police commissioner shared the ACLU's concerns that this would allow officers "an opportunity to shape their accounts around what the recording showed."[12] Lack of guidelines for release of the footage also "rais[ed] concerns for accountability since the public was not guaranteed any degree of access."[13] The perceived flaws in this implementation caused the ACLU to publicly withdraw support for the entire Los Angeles program, claiming that many of these practices undermined the purpose of using body cameras.[14] This incident illustrated an important concern with body camera programs: absent the right policies, the technology may be used to tailor narratives or gather evidence of routine criminal activity instead of ensuring police accountability,[15] thus introducing privacy concerns while failing to assure the public that body cameras will help to curb abuse. The controversy over the LAPD program illuminated the important and sensitive concerns behind the expansion of such programs, revealing that body cameras may fail to serve the public unless accompanied by carefully crafted policies that can help to realize their potential benefits and contain the risks.

Privacy and accountability are the primary interests implicated with body camera use, and policies must adequately protect both interests for implementation to actually benefit the public. The current dialogue, however, misunderstands how certain policies affect these interests because of a misconceived framing of the problem as a privacy-accountability dichotomy. The principal

---

10. *See id.*

11. *See id.* (noting also that some officials claimed that such review could be denied in use-of-force incidents, but this was not codified in the actual policy).

12. *Id.*

13. *Id.*

14. *See id.*; *see also* Kate Mather, *ACLU to Justice Department: Don't Give LAPD Money for Body Cameras*, L.A. TIMES (Sept. 3, 2015), http://www.latimes.com/local/lanow/la-me-ln-aclu-lapd-body-cameras-20150903-story.html [https://perma.cc/RTS6-JHK7].

15. *See* Open Letter from Denise E. O'Donnell, Bureau of Justice Assistance, ACLU of Southern California (Sept. 3, 2015), http://www.aele.org/aclu2doj-lapd$.pdf [https://perma.cc/QVU2-R4ED] [hereinafter "ACLU Letter to DOJ"] ("The body-worn camera program implemented by LAPD's policy is very different from the kind of program contemplated by the DOJ. . . . Section I of the policy, which lays out the objectives of the program, focuses explicitly on gathering evidence of crime, 'deter[ring] criminal activity and uncooperative behavior during police-public interactions,' assisting officers with completing reports, assisting in the resolution of complaints 'including false allegations by members of the public' and providing other information for officer 'evaluation training and improvement.'" (citation omitted)).

flaw with this perspective is that it overstates the privacy harms tied to body camera use and therefore significantly disservices policymaking. This privacy impact is miscalculated, both because privacy harms are assumed to be mostly inevitable and because the privacy benefits that can accompany body camera programs (such as fewer privacy violations resulting from police misconduct) are not given adequate weight. In reality, body camera programs can implicate various privacy interests in complex ways. A framework centered on a more-complete view of these privacy issues would allow for more-thoughtful insight into how policies can best serve these privacy interests.

This Note will consider privacy benefits accompanying body camera programs in order to construct a more-complete account of the privacy side of the body camera analysis, then discuss how policies consistent with a privacy-oriented approach could maximize privacy benefits while mitigating the harms. With this more-comprehensive view of affected privacy interests, police departments will be able to craft policies that better defend and enhance civilians' privacy interests.

II. UNDERSTANDING THE PRIVACY SIDE OF THE EQUATION

Despite overwhelming public support for body cameras,[16] threats to civilian privacy from body camera usage present a significant concern; both advocates and critics fear that more recording means less privacy.[17] Some perceive this privacy concession as the price necessary for the desired increase in official accountability and reduction in police misconduct, since cameras would move police interactions into a documented and more-public sphere.[18] This view relies on an assumed tradeoff, wherein more

16. In a poll from YouGov, 88% supported "a proposal for police officers to wear body cameras" (with 8% opposing and 4% not sure). YOUGOV, POLL 2 (Apr. 27–29, 2015), *available at* http://cdn.yougov.com/cumulus_uploads/document/rcrwgep1rx/tabs_OPI_police_body_cams_20150429.pdf [https://perma.cc/4VK2-345S].

17. *See, e.g.*, Matt Pearce, *Growing Use of Police Body Cameras Raises Privacy Concerns*, L.A. TIMES (Sept. 27, 2014), http://www.latimes.com/nation/la-na-body-cameras-20140927-story.html [https://perma.cc/5LQ8-9LVB] ("[E]quipping police with such devices also raises new and unsettled issues over privacy at a time when many Americans have been critical of the kind of powerful government surveillance measures that technology has made possible."); Tanzina Vega, *Rights Groups: Police Use of Body Cameras Raises Privacy Concerns*, CNN (May 15, 2015), http://www.cnn.com/2015/05/15/politics/body-cameras-civil-rights-privacy-coalition [https://perma.cc/S3E5-XFWL].

18. *See, e.g.*, Harvard Law Review Ass'n, *Considering Police Body Cameras*, 128 HARV. L. REV. 1794, 1808 (2015) ("[I]ncreasing transparency necessarily means more

accountability inevitably requires a loss of privacy as the cost. However, if privacy interests are not necessarily forfeited as cameras become more prominent, then the privacy side of the equation requires a more-complex evaluation in policymaking. This Part's more-thorough account of how body cameras can affect privacy interests will reveal that different kinds of privacy harms and benefits are implicated, and that privacy is not mutually exclusive with increased accountability, because increased accountability can itself create privacy benefits. Therefore, discussion of body camera implementation and policy must move beyond the conventional view that more body cameras necessarily entails less privacy and consider both the positive and negative effects on privacy interests. This understanding is essential in creating policies that best serve the public.

A. PRIVACY HARMS

Body cameras undoubtedly present risks to civilians' privacy. The subjects of police encounters are most obviously affected by the use of devices that record and preserve video evidence of those encounters, because officers' interactions with these people will likely be most direct and invasive (especially if the person is searched, arrested, or confronted in a private setting, for example). The subject of an investigation may not be in public during a police encounter, so body cameras could record individuals in settings that were meant to remain private. Even in public, the subject could be required to disclose information to the police about his or her private life or whereabouts that could lead to embarrassment if disseminated. For these individuals, the interplay between privacy and security is most apparent: the recording of this encounter may prevent police misconduct, but comes at the price of footage that may be viewed by others, including the police or even the public. These concerns are exacerbated during an illegal search, where the officers on scene are not even lawfully intruding on the subject's private sphere, but body cameras now extend the number of onlookers observing this legally protected area to anyone who watches the footage.[19]

---

people will view body-camera footage, which will frequently feature civilians who may not want the recordings of themselves shared.").

19. This may be the case during illegal searches of the home and person, including unlawful stop-and-frisk encounters. The harm in these circumstances, where the very

Body camera usage affects the privacy interests of many more people than the direct subjects of investigation, however.[20] Bystanders or passersby, whether involved with the subject of an encounter or not, will inevitably be captured on a large number of recordings in both public and private settings, perhaps unaware that the police are filming.[21] Victims of crimes or accidents who need police assistance or are questioned by police will find themselves recorded more regularly, even if a threshold policy is established to cease recording under certain conditions.[22] Individuals who converse with police officers outside of the investigation context — such as to report crimes, provide information, or simply speak without an official purpose — may be recorded as well.

Additional concerns for the general public include the use of the footage to conduct dragnet surveillance, whereby evidence is collected and reviewed without judicial supervision or any basis of suspicion.[23] This concern is substantially greater if facial-

---

encounter is a privacy violation, is compounded when a body camera records the encounter and perhaps subjects it to viewing and dissemination.

20. There is debate over the privacy of police officers who are required to use body cameras while on duty in addition to the concerns about civilians' privacy. *See* Matthew Feeney, *Police Body Cameras Raise Privacy Issues for Cops and the Public*, CATO INST.: CATO AT LIBERTY (Feb. 12, 2015), http://www.cato.org/blog/police-body-cameras-raise-privacy-issues-cops-public [https://perma.cc/245R-USEH] ("While it is technically possible for officers with body cameras to have the devices on throughout a shift, there are serious problems with this requirement. . . . [P]olice officers deserve some privacy while on the job. . . . [I]t remains the case that police officers ought to be able to talk to each other in cruisers about department gossip and other topics without fear that members of the public may request footage of the conversation.").

This Note will, however, limit discussion to the privacy of individuals who are not on-duty law enforcement officials acting on behalf of the government. Concerns of police-officer privacy may be better managed through internal recording policies.

21. *See* ACLU RECOMMENDATIONS, *supra* note 4, at 3 ("Continuous recording would also mean a lot of mass surveillance of citizens' ordinary activities. . . . [I]n a place like New York City it would mean unleashing 30,000 camera-equipped officers on the public streets, where an officer on a busy sidewalk might encounter thousands of people an hour. That's a lot of surveillance.").

22. For a discussion about concerns with the number of innocent people recorded with body cameras in place, see Eileen Sullivan, *Police Body Cameras May Solve 1 Problem But Create Others for Victims and Innocent Bystanders*, ASSOCIATED PRESS (Sep. 11, 2015), http://www.usnews.com/news/politics/articles/2015/09/11/police-body-cameras-may-solve-one-problem-but-create-others [https://perma.cc/6R33-AV8R] ("While the recordings may help get to the truth of an incident with police, they also record distraught victims, grieving family members, people suffering from mental illness and citizens exercising their rights to free speech and civil disobedience. Cameras may solve one problem but create others.").

23. Dragnet law enforcement in the technological context is, generally speaking, "surveillance of any citizen . . . without judicial knowledge or supervision," as opposed to simply "enabl[ing] the police to be more effective in detecting crime." United States v. Knotts, 460 U.S. 276, 283–84 (1983) (citation and internal quotation marks omitted). For

recognition technology can be applied to existing footage, which could allow for local, state, or federal agencies to keep records of the location of any individual whose face is on the footage.[24] Because it would be difficult or even impossible for the public to verify whether dragnet-policing practices exist, the threat itself may still damage the public's sense of privacy.[25]

Many of these risks can be assuaged by sensible policies for the appropriate use of such cameras. For example, policies regulating when cameras should be recording, which have been the subject of much recent discussion, will likely help to minimize various privacy risks.[26] Other risks could be mitigated by better control over how footage is stored, used, and accessed. Even with policies in place to manage privacy risks, however, recording will

---

a discussion of dragnet policing concerns arising from body cameras and facial recognition technology, see Kelly Freund, Note, *When Cameras are Rolling: Privacy Implications of Body-Mounted Cameras on Police*, 49 COLUM. J.L. & SOC. PROBS. 91, 103–05 (2015); *see also* ACLU Letter to DOJ, *supra* note 15, at 8–9 ("[I]f new technology is adopted without appropriate safeguards, it can quickly backfire. The prospect that facial recognition technology could be used in conjunction with body-worn camera video threatens to turn tools meant to promote police accountability into tools for mass surveillance."). Recent practices such as the LAPD's use of body camera footage to review incidents before writing a report exacerbates these concerns. *See* Mather, *supra* note 9.

24. *See* Freund, *supra* note 23, at 103–05; Shakeer Rahman, *Body Cameras Could Transform Policing — for the Worse*, AL JAZEERA AM. (Apr. 17, 2015), http://america.aljazeera.com/opinions/2015/4/body-cameras-could-transform-policing--for-the-worse1.html [https://perma.cc/E3GX-C8JH].

25. "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring). For a discussion of the specific privacy harms that result from general surveillance and how they diminish privacy and impact autonomy, see Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000). Privacy harms are not limited to when actual observation or disclosure of private information is revealed to the public, but fear of observation itself diminishes the separation of public and private life. *Id.* at 1425–26 ("The injury . . . does not lie in the exposure of formerly private behaviors to public view, but in the dissolution of the boundaries that insulate different spheres of behavior from one another. The universe of all information about all record-generating behaviors generates a 'picture' that, in some respects, is more detailed and intimate than that produced by visual observation, and that picture is accessible, in theory and often in reality, to just about anyone who wants to see it.").

Even if these activities take place in a public setting, memorializing them and making them freely accessible to the police can still be deleterious to privacy. *Cf.* Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 113–14 (2008) (critiquing the principle adopted by courts that voluntarily turning over information to third parties opens that communication to government monitoring, and identifying the significant risks to legal protections of privacy that follow such reasoning).

26. The ACLU has focused heavily on recording policies as a means to protect privacy. *See* ACLU RECOMMENDATIONS, *supra* note 4. For a discussion of these and other prominent recommendations around recording policies, see Freund, *supra* note 23, at 116–24.

still take place, so the proliferation of body cameras will necessarily result in more recording of individuals in public and private places than if the police did not employ body cameras. These privacy harms increase substantially when police have complete discretion as to when they review footage or release it to the public.[27] Even if footage is never actually viewed, however, the act of recording and memorializing a person's activities may itself constitute a privacy harm,[28] and thus even a perfect policy regime would still entail some privacy harms.

In light of these various privacy risks, many see the issue of body cameras as a privacy-versus-security problem.[29] The key question under this approach would thus be whether the benefits of reduced police misconduct outweigh these privacy harms. While advocates have concluded that these risks can be properly contained with the right policies, which would justify the use of body cameras despite the perceived costs,[30] the calculus may nevertheless be flawed by an assumption that body cameras affect privacy interests in a strictly negative way. It is thus essential to approach policymaking with a view toward not merely mitigating privacy risks, but balancing them against the privacy benefits.

B. PRIVACY BENEFITS

Framing body camera policy as merely a tradeoff between privacy harms on the one hand and accountability benefits on the other takes an overly narrow view that privacy interests can only be affected negatively by body camera proliferation.[31] This view

27. *See* ACLU Letter to DOJ, *supra* note 15, at 5 ("LAPD's refusal to set forth clear policies on the public release of video also creates the impression it may release video that exonerates officers but not video that shows misconduct. That approach will undermine rather than advance public trust in police. . . . [W]hile the policy bars unauthorized release of video by officers, its failure to set any rules for release through authorized channels threatens privacy by potentially allowing release of sensitive or embarrassing footage where there is no clear public interest in disclosure.").

28. Even if recordings are never actually disclosed or shared, the record and accessibility of the information itself causes the subject to shape his or her decision-making. *See* Cohen, *supra* note 25, at 1425–26.

29. *See, e.g.*, Pearce, *supra* note 17 (noting "issues of privacy" as the cost of monitoring police activity); ACLU RECOMMENDATIONS, *supra* note 4, at 2 ("[T]he challenge of on-officer cameras is the tension between their potential to invade privacy and their strong benefit in promoting police accountability.").

30. *See supra* note 5 and accompanying text.

31. This implicit assumption appears in much of the discussion where protection of privacy is achieved only by limiting the recording that occurs. *See* ACLU RECOMMENDATIONS, *supra* note 4, at 3 ("Purely from an accountability perspective, the

fails to properly assess the overall utility of body cameras or particular policies, because it excludes from the calculus the privacy benefits that may result from more recording. These benefits are vital to this consideration, because they substantially reduce the net privacy harm incurred by increased body camera presence.

Privacy benefits from the increased use of body cameras can be realized in three principal ways. First, if body cameras fulfill their promise to deter police misconduct, including illegal arrests and detentions, individuals will be freer from privacy violations by law enforcement both in public and in private places. Body camera usage may help reduce illegal searches, for instance, as footage may prove lack of requisite cause for past searches and deter similar future conduct. In turn, this deterrent effect will benefit the privacy of individuals who may be subject to such unlawful encounters, because every illegal search or seizure prevented protects the individual from the privacy loss that would have accompanied such an infringement. Second, once privacy-infringing conduct on the part of police is deterred more effectively, decreases in both the actual and perceived level of police misconduct will result in more public trust in law enforcement.[32] In practice, body camera programs in many departments have indeed led to a drop in civilian complaints of misconduct.[33] Greater

ideal policy for body-worn cameras would be for continuous recording throughout a police officer's shift, eliminating any possibility that an officer could evade the recording of abuses committed on duty. The problem is that continuous recording raises many thorny privacy issues, for the public as well as for officers.").

32. *See, e.g.*, TRACEY MEARES & PETER NEYROUD, RIGHTFUL POLICING 5–7 (Nat'l Inst. of Justice & Harvard Kennedy Sch.'s Program in Criminal Justice Policy and Mgmt. eds., 2015) ("Research shows that people are motivated more to comply with the law by the belief that they are being treated with dignity and fairness than by fear of punishment. In fact, being treated fairly is a more important determinant of compliance than formal deterrence. . . . All of this encourages desistance from offending, law-abiding and assistance to the police, contributing to lower crime rates."); Tom R. Tyler, Phillip Atiba Goff & Robert J. MacCoun, *The Impact of Psychological Science on Policing in the United States: Procedural Justice, Legitimacy, and Effective Law Enforcement*, 16 PSYCHOL. SCI. PUB. INT. 75 (2015) ("[L]egitimacy — that is, public trust and confidence — can be an important factor in policing and that a focus on legitimacy provides an additional motivational force that lowers crime."); *see also* Neill Franklin, *Body Cameras Could Restore Trust in Police*, N.Y. TIMES (Oct. 22, 2013), http://www.nytimes.com/roomfordebate/2013/10/22/should-police-wear-cameras/body-cameras-could-restore-trust-in-police [https://perma.cc/8TPG-ZWV3] ("The infamous 'blue wall of silence' — the tendency of police to defend against any accusations of wrongdoing — has compounded the problem. But by adopting an objective, transparent monitoring system that allows us to defend those unjustly accused and correct or punish those caught abusing their power, we can prove to the public we believe no person should be above the law, particularly those sworn to uphold it.").

33. *See, e.g.*, Leila Atassi, *Cleveland Police Body Cameras Reduced Citizen Complaints by 40 Percent, Police Officials Say*, CLEVELAND.COM (Nov. 11, 2015),

levels of trust between police departments and a community can lead to more-effective policing and prevention of crime,[34] which in turn enhances the privacy of civilians by reducing the prevalence of privacy-infringing crime, such as burglary and stalking. Third, if a body camera happens to record evidence of a crime that violates a victim's privacy, the footage can then aid in prosecution of that person, and ultimately his or her punishment and incapacitation.[35] Additionally, even members of the public who would not have otherwise been subject to actual privacy violations benefit indirectly from the above effects of body cameras: the very threat of unwarranted surveillance or privacy-infringing activity, including crime, affects the decision-making process of the individual, constraining autonomy and the ability to feel secure in one's private activities.[36] Thus, reasonable fear of unchecked privacy violations at the hands of law enforcement or government itself threatens privacy by creating a perpetual entry point into the

---

http://wwwcleveland.com/cityhall/index.ssf/2015/11/cleveland_police_body_cameras_1.html [https://perma.cc/QMN4-DNXN] ("[C]itizen complaints against officers have dropped nearly 40 percent since the department began using body-worn cameras . . . ."); Rory Carroll, *California Police Use of Body Cameras Cuts Violence and Complaints*, GUARDIAN (Nov. 4, 2013), http://www.theguardian.com/world/2013/nov/04/california-police-body-cameras-cuts-violence-complaints-rialto [https://perma.cc/7XLG-R9MX] (In one city, "after cameras were introduced in February 2012, public complaints against officers plunged 88% compared with the previous 12 months. Officers' use of force fell by 60%."); Tony Perry, *San Diego Police Body Camera Report: Fewer Complaints, Less Use of Force*, L.A. TIMES (Mar. 18, 2015), http://www.latimes.com/local/lanow/la-me-ln-body-cameras-20150318-story.html [https://perma.cc/63LM-THBC] ("Complaints have fallen 40.5% and use of 'personal body' force by officers has been reduced by 46.5% and use of pepper spray by 30.5% . . . ."); Carol Robinson, *Birmingham Police Body Cameras Bring Drop in Use of Force, Citizen Complaints*, AL.COM (Sept. 14, 2015), http://www.al.com/news/birmingham/index.ssf/2015/09/birmingham_police_body_cameras_1.html [https://perma.cc/7NHS-4P6R] ("For the months of July and August, use of force incidents dropped 34 percent and citizens' complaints dropped 70 percent."); Nick Wang, *Study Shows Less Violence, Fewer Complaints When Cops Wear Body Cameras*, HUFFINGTON POST (Oct. 13, 2015), http://www.huffingtonpost.com/entry/police-body-camera-study_us_561d2ea1e4b028dd7ea53a56 [https://perma.cc/FU95-JPEN] (After the Orlando Police Department's twelve-month trial, "use-of-force incidents . . . dropped 53 percent among officers with the cameras. Civilian complaints against those officers also saw a 65 percent decline.").

34. *See* David Hudson, *Building Trust Between Communities and Local Police*, WHITE HOUSE BLOG (Dec. 1, 2014, 8:25 PM), https://www.whitehouse.gov/blog/2014/12/01/building-trust-between-communities-and-local-police [https://perma.cc/NW3D-3P7H] (discussing body cameras as part of a plan "to promote expansion of the community-oriented policing model, which encourages strong relationships between law enforcement and the communities that they serve as a proven method of fighting crime"). For a discussion of community policing, see generally BUREAU OF JUSTICE ASSISTANCE, UNDERSTANDING COMMUNITY POLICING: A FRAMEWORK FOR ACTION (1994).

35. For a discussion of when the use of such footage should be permitted, see *infra* Part IV.B.

36. *See* Cohen, *supra* note 25.

private sphere. Eliminating such continual concerns is a substantial benefit to all civilians, not only would-be victims of misconduct.

The prevailing account of body cameras fails to consider the above privacy benefits, among other indirect benefits, which distorts the views of policymakers by casting the net impact of body cameras on privacy in an artificially strong negative light. This is largely attributable to the fact that these benefits take a different form than the more-apparent harm an individual experiences when subjected to more recording and monitoring. This miscalculation is a specific instance of a phenomenon, termed "privacy-privacy tradeoffs" by Professor David Pozen,[37] whereby policymakers often exercise flawed logic when discussing privacy because the privacy risks of a new policy may appear in a different form than the benefits sought, or vice versa.[38] In other words, a privacy interest affected by a certain policy may look very different than the one most obviously implicated, and thus the former may be overlooked or underappreciated because the impact is not as clear or is unexpected. Privacy interests implicated by a particular policy may vary in form by, for example, implicating different interests, affecting different parties, or affecting parties at different times.[39] Professor Pozen discusses two examples: (1) police profiling, which may reduce privacy for one group who is subjected to more searches while increasing privacy for the rest of the population,[40] and (2) the TSA's "PreCheck" program, which allows passengers to trade information about themselves at one point in time for less-thorough screening at later times.[41] This theory provides a framework for better understanding the relationships among the various privacy interests associated with body cameras and helps to explain why some privacy benefits have gone underappreciated.

These privacy-privacy tradeoffs are apparent in the context of body cameras, even though they are currently overlooked. The use of body cameras entails dynamic tradeoffs, meaning that the harm and benefit occur at different times.[42] The privacy benefits

37. This phenomenon of privacy interests implicated in a policy taking different forms is set forth in David Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221 (2015).
38. *Id.* at 223.
39. *Id.* at 227–31.
40. *Id.* at 229.
41. *Id.* at 222.
42. *See id.* at 229 (Dynamic tradeoffs "shift privacy risk across time periods.").

discussed above will largely occur after more-effective oversight has had time to take effect, because deterrence and improved community attitudes will not be instantaneous. Thus, fearing only the immediate privacy harms that may accompany increased use of this technology, however warranted, provides an incomplete assessment of net privacy impact without looking to how potential benefits will accrue over time. Body cameras also implicate dimensional or domain tradeoffs, in which different privacy interests are traded.[43] The privacy benefits obtained from fewer illegal searches and reduced fear of privacy violations from the police, as well as those associated with more-effective policing and higher assurance of effective crime prevention, involve a sense of security of one's person, home, and physical freedom; these privacy concerns are different in type than the harm that results from increased observation, as the latter does not involve this physical intrusion. Just as these kinds of tradeoffs impair policymakers from fully understanding privacy effects in other contexts, they likely explain the failure to understand the privacy benefits in the body camera context.

Policymakers must understand these tradeoffs and consider how they affect the net privacy effect of body cameras. The prevailing policy recommendations may be suboptimal because these policies do not work to fully account for the potential privacy benefits and how much they offset the risks. By viewing privacy not as a monolith but as a multifaceted concept and a complex part of the equation, policymakers may grasp a more-complete account of the effects of body cameras on the public, thus leading to better-informed policies.

C. CRAFTING POLICY WITH A FOCUS ON NET PRIVACY IMPACT

In order to ensure that body camera programs develop to best serve privacy and accountability interests, policymakers should adopt this more-complex view of the privacy impact of body cameras and should carefully assess both the privacy harms and benefits of any rules governing their use. Through this perspective,

43. *See id.* at 230–31 (Dimensional tradeoffs "shift risk across different privacy interests. . . . [W]hen the traded-off risks are understood to be not just factually but qualitatively distinct from or even incommensurate with each other, we might say that a dimensional tradeoff rises to the level of a *domain tradeoff*. The privacy interests on either side of the ledger, in such a case, seem to implicate different domains of value.").

policymakers can understand that body cameras provide an even greater utility than a more-simplistic view would indicate. A framework that so encompasses all kinds of privacy interests would better guide development of policies that optimize the net privacy impact while preserving the accountability function.

To craft policies that achieve this goal, privacy must be considered on two fronts: minimizing harms and maximizing benefits. However, discussion has primarily focused on harm reduction[44] to the exclusion of recognizing privacy benefits that accrue in other forms. A policy regime must therefore manage the process of recording, handling, editing, and accessing footage in a manner that contemplates both the risks and benefits to privacy. Such a policy regime would support the expanded use of body cameras both in terms of accountability and privacy.

In light of these various ways in which privacy can be affected, this Note argues that the policies needed to ensure that body camera systems are implemented with the best possible net privacy impact must therefore meet several criteria. Broadly, they must not compromise the public's ability to monitor police misconduct: they must ensure that police encounters are recorded when appropriate, that footage of these encounters is stored and managed reliably, and that this footage is accessible to courts or the public when necessary to expose misconduct. The policies must also limit (1) recording of civilian activity, (2) disclosure of footage to situations in which accountability and privacy interests are best served, and (3) the potential (and the perceived potential) for government officials to abuse their access to the footage. In contrast to the narrow view of a strict privacy-accountability tradeoff, focusing on the net privacy impact (by seeking both to reduce privacy harms and bolster privacy benefits) will better guide policymakers to achieve these goals.

These considerations should guide how body cameras and their footage are used at each step of the process, from recording to eventual deletion or release (whether to the public, to a law-enforcement agency, or to a court). Relations between the American public and law enforcement are at a pivotal point in which body cameras are being used with increasing frequency — a trend that does not appear to be slowing.[45] Body camera policies across

44. *See supra* note 31 and accompanying text.

45. *See* Jeremy Gorner, *Chicago Police Expanding Body Cameras to Six More Districts*, CHI. TRIB. (Dec. 23. 2016), http://www.chicagotribune.com/news/local/breaking/

the nation are varied and shifting, as different groups seek to maximize what they perceive as the primary function of the technology.[46] Adopting a comprehensive, privacy-focused framework for developing these policies is thus essential to realizing the potential of body cameras to best serve the public, both by protecting privacy interests and protecting against official misconduct.

A privacy-based approach may be particularly important for developing policies with respect to handling footage after a recording takes place,[47] because the actual and potential ways the fruits of this technology are used will determine the way and degree to which these privacy interests are affected. The remainder of this Note will thus consider how net privacy effects can be optimized specifically through policies governing how footage is stored and how it can be accessed.

III. ENTRUSTING THE FOOTAGE

Currently, police agencies generally manage the storage and access of their own footage.[48] The most-prominent policy recommendations do not challenge this practice.[49] A privacy-oriented approach, however, reveals serious concerns with such a system.

---

ct-chicago-police-body-cameras-met-20151223-story.html [https://perma.cc/HZ48-GQHX] (discussing expansion of Chicago's test program after a dash-cam video showed an officer shooting Laquan McDonald sixteen times); *see also* Dep't of Justice, *supra* note 2 (announcing the approval of a nationwide funding initiative for increased use of body cameras); Nelson & Tau, *supra* note 2 (discussing President Obama's call for more body cameras).

46. For example, while the ACLU prioritizes accountability, *see* ACLU RECOMMENDATIONS, *supra* note 4, law-enforcement officials have begun tapping into uses for body cameras more valuable for their own roles. *See* ACLU Letter to DOJ, *supra* note 15.

47. Further, policy recommendations for when recording should actually take place are discussed extensively elsewhere. *See supra* note 26.

48. No examples could be found of police departments that were restricted, either by law or practice, from how the footage must be stored or when it could be accessed by law enforcement.

49. No serious consideration or recommendation of outsourcing or otherwise moving storage of footage outside of police departments' control could be found. *See* ACLU RECOMMENDATIONS, *supra* note 4; LINDSAY MILLER ET AL., IMPLEMENTING A BODY-WORN CAMERA PROGRAM: RECOMMENDATIONS AND LESSONS LEARNED 15–16 (2014) (noting under its data storage policy recommendations that, among forty departments consulted, "all [departments] stored body-worn camera video on an in-house server (managed internally) or an online cloud database (managed by a third-party vendor)," but not challenging unrestricted access to footage by the department). While the ACLU does express concern about editing or manipulating footage, it targets most of its focus on the actual recording process and does not go as far as to suggest actually removing police departments' capability to review footage. *See* ACLU RECOMMENDATIONS, *supra* note 4.

The purpose of retaining body camera footage is to document and deter misconduct by law-enforcement officials. If those very officials are able to handle and control the footage, members of the public may perceive a potential conflict of interest, which may very well erode trust that the program will effectively oversee those officials and hold them accountable. If body cameras fail to fulfill their promise of increased accountability and the public has little faith in the safeguards against misuse of footage, this failure will undermine the potential privacy benefits and unnecessarily impose privacy risks. Instead, policymakers can avoid these problems by implementing alternatives such as private third-party management of footage, thus preserving the privacy benefits and accountability goals of body cameras.

A. ISSUES WITH POLICE-DEPARTMENT MANAGEMENT OF FOOTAGE

The management of body camera footage by local police departments presents serious risks and harms to the privacy interests of civilians, even if the footage is not physically stored on site. Current recommendations either fail to consider these privacy implications or deem them practically inevitable, because no prominent policy recommendations seem to challenge this practice. These harms take two principal forms.

First, footage may be improperly released for a variety of illegitimate purposes. Footage could potentially be leaked, for example, in an attempt to embarrass or discredit an individual who had a negative experience with law enforcement.[50] This very possibility harms citizens' privacy interests, because potential claimants of police misconduct may fear that compromising footage of their private lives will find its way into the public eye in retaliation, and they may conduct themselves differently than they would were they free from state intrusion into their lives.[51] These privacy harms are significant even if scenarios such as these

50. *See* ACLU RECOMMENDATIONS, *supra* note 4, at 5 ("In the case of dashcams, we have also seen video of particular incidents released for no important public reason, and instead serving only to embarrass individuals. Examples have included DUI stops of celebrities and ordinary individuals whose troubled and/or intoxicated behavior has been widely circulated and now immortalized online. The potential for such merely embarrassing and titillating releases of video is significantly increased by body cams." (citations omitted)).

51. *See supra* note 25 and accompanying text.

do not actually occur often, because just the possibility of retaliation presents an ongoing fear to those who are recorded in private situations.[52] Thus, even if policies exist to deter improper release of footage, the ease of both accessing and viewing body camera footage creates significant risks to privacy as well as real, ongoing harms.

Second, because of the lack of oversight over the storage and viewing of body camera footage, police departments may find it easier to both engage in and normalize dragnet-policing tactics, whereby footage is aggregated and reviewed to find new evidence of previously undiscovered and unsuspected criminal activity.[53] This substantially elevates whatever harms inhere in the mere recording of personal activity, because law enforcement can review footage for intimate or incriminating details that may not have been observed in the course of regular police activity; these include intricate details of the inside of one's home, the identities of passersby on the street who may not have been aware that recording was taking place, items in a car not fully observed on first glance, and activity viewable through every open window within view. With the ability to review footage at will comes the power to comb through the background for these details, noticing or reexamining even innocent activity (including the behavior of victims of crimes, whose privacy may have already been harmed once by being recorded in a vulnerable state). This could allow those viewing the footage to create intimate and detailed profiles of people beyond the level possible by mere real-time observation.[54]

Together, these possibilities demonstrate the significant privacy harms created by the status quo for footage storage and management. To obtain a complete picture of the privacy impact caused by this practice, however, the effect on privacy benefits must be considered as well.

The privacy benefits of body cameras take several forms, but they generally stem from the potential of the cameras and poli-

52. Knowledge that recordings could be used in these ways entails its own privacy harm, as individuals remain aware that their activity could be disclosed at virtually any time. *See supra* note 25 (discussing how surveillance and recording can themselves harm privacy, even if this observation is merely suspected).

53. *See* Freund, *supra* note 23, at 121.

54. *See supra* note 25 (discussing why recording and reviewing footage of private activities harms privacy beyond firsthand observation).

cies to capture and deter misconduct.[55] Law-enforcement agencies exercising virtually unchecked control over their own footage undermines that potential for effective oversight and thus diminishes the positive privacy impact of body cameras. One way in which this occurs is evinced by the LAPD's controversial practice of having officers review footage of an encounter before writing a report.[56] This practice has been criticized for allowing officers to frame potential instances of misconduct in a manner consistent with the video instead of using the footage to verify an original account.[57] Allowing an officer to frame the narrative of an incident consequently hampers the privacy benefits of body cameras, because as critics have observed, the deterrent against misconduct is diminished when officers who fear discipline could review the footage and construct a post hoc justification for the actions consistent with the footage (which will in many cases be the only evidence of the encounter aside from the testimony of the complaining civilians).[58] Even absent a policy of reviewing footage before writing an official report, some may worry that officers fearing a complaint could watch footage to preemptively develop an account of an incident that deflects responsibility for misconduct.[59] Though there may be legitimate ends to such review — such as increasing the accuracy of reports and the depth of investigations — it is difficult to justify such methods in the face of increased recording unaccompanied by publicly trusted oversight. Because of these potential threats to accountability, police-department management of footage may thus foreclose a large

55. *See supra* Part II.B (evaluating privacy benefits of body cameras).

56. *See* Mather, *supra* note 9.

57. *See id.*; ACLU Letter to DOJ, *supra* note 15, at 6 ("[A]llowing officers to review footage before making an initial statement threatens to taint investigations, undermines the use of body-worn cameras as a tool for accountability, and hurts the public trust that body-worn cameras should be building. . . . By providing an objective record of an incident, body-worn cameras can lessen an investigation's dependence on the officer's account and the officer's credibility, helping restore confidence in the investigative process even for those that may not trust individual officers to be fully truthful. But allowing officers under investigation to view video before making a statement about a critical incident undermines this effort by providing officers who are inclined to lie the opportunity to do so in a manner consistent with the video evidence.").

58. *See* Mather, *supra* note 9; ACLU Letter to DOJ, *supra* note 15, at 6 ("Police departments know that showing video to witnesses threatens to taint their testimony, because they do not do so in any other situations, including with other witnesses to police shootings.").

59. *See* Mather, *supra* note 9 (discussing the LAPD's policy of reviewing footage before writing reports).

degree of the privacy benefits that would result from increased public trust and reduced misconduct.

By failing to take into account privacy benefits as well as harms, policymakers may be unaware of, and therefore may underestimate, the harm caused by current practices. Therefore, such policymakers perpetuate the notion that privacy must be sacrificed to avoid police misconduct by advertising current practices as what the public must give up at the cost of official accountability. In reality, acknowledging the privacy benefits of body cameras would mean that the public is simply managing its privacy interests by engaging in a more-nuanced tradeoff across temporal and qualitative realms. The latter view provides a much stronger case for embracing body cameras, but it also demands that for issues as important to privacy as who controls the footage, policymakers thoroughly consider how potential policy choices can affect these interacting privacy interests. Alternative policy regimes such as the one this Note suggests may allow the public to embrace body cameras as a beneficial rearrangement of privacy interests and not a necessary evil.

B. EXCLUSIVELY PRIVATE CONTROL AS AN ALTERNATIVE

Existing legal strategies used to protect privacy in other contexts can be used to avoid the problems caused police departments handling their own footage. Because the privacy harms and foregone privacy benefits discussed above stem from the fact that law enforcement has control over its own body camera footage, exclusive storage by a private third party is a feasible alternative that would mitigate or even remedy this net privacy loss. While such a system would present its own concerns, a privacy-centered perspective suggests that management by a private party would better serve individuals captured by body cameras than the status quo.

Third-party entities have been used in other contexts to store information that could be misused when managed by government agencies. In 2014, the President's Review Group on Intelligence and Communications Technologies recommended that telephone metadata collected under Section 215 of the USA Patriot Act[60] be

60. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered titles of U.S.C.) [hereinafter "Patriot Act"].

stored with either the phone carriers or a third party.[61] The reason for this recommendation was:

> Knowing that the government has ready access to one's phone call records can seriously chill "associational and expressive freedoms," and knowing that the government is one flick of a switch away from such information can profoundly "alter the relationship between citizen and government in a way that is inimical to society." That knowledge can significantly undermine public trust, which is exceedingly important to the well-being of a free and open society.[62]

The USA Freedom Act[63] — the law that replaced the Patriot Act in 2015 — ultimately did not use entirely independent third parties to store telephone data, but instead left the metadata in the control of the private carriers, subject to query.[64] Still, the rationale of the President's Review Group and the actual imple-

---

61. "We recommend that legislation should be enacted that terminates the storage of bulk telephony meta-data by the government under section 215, and transitions as soon as reasonably possible to a system in which such meta-data is held instead either by private providers or by a private third party . . . ." THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 25 (2013), *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [https://perma.cc/Z4Z9-U89R]; *see also id.* at 119 ("If reliance on government queries to individual service providers proves to be so inefficient that it seriously undermines the effectiveness of the program, and if the program is shown to be of substantial value to our capacity to protect the national security of the United States and our allies, then the government might authorize a specially designated private organization to collect and store the bulk telephony meta-data.").

62. *Id.* at 117 (quoting United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring)).

63. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) [hereinafter "Freedom Act"].

64. *See id.*; *see also Summary: H.R. 2048 — 114th Congress (2015–2016)*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/2048 [https://perma.cc/BP8R-GZD6] (last visited Nov. 26, 2016) (providing a summary of the Freedom Act); Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 is Sharply Limited*, N.Y. TIMES (June 2, 2015), http://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html [https://perma.cc/ZUQ9-ADE2] ("The [Freedom Act] signaled a cultural turning point for the nation, almost 14 years after the Sept. 11 attacks heralded the construction of a powerful national security apparatus. The shift against the security state began with the revelation by Edward J. Snowden, a former National Security Agency contractor, about the bulk collection of phone records. The backlash was aided by the growth of interconnected communication networks run by companies that have felt manhandled by government prying. The storage of those records now shifts to the phone companies, and the government must petition a special federal court for permission to search them.").

mentation of private storage demonstrate that third-party storage and management of body camera footage may be a realistic and rational solution to concerns about government control of sensitive personal data.

The concern with unfettered government access to body camera footage is significantly greater than with metadata, because actual footage captures more detail in a more-personal way than mere data, and thus the case for entrusting a third party is even stronger here than in the phone data context. The President's Review Group noted, citing Justice Sotomayor's concurring opinion in a case involving GPS monitoring, that metadata could be particularly concerning if revealing sensitive information pertaining to the subject's medical, religious, sexual, and familial details.[65] Here, the police could use body camera footage to readily determine personal characteristics of the filmed individuals with ease and actually observe private activity firsthand. Police encounters may frequently take place at particularly sensitive moments and in private settings, and the footage obtained can provide evidence about a person's private life far beyond the inferences allowed by metadata. For instance, studies have shown that metadata can very easily reveal information such as medical issues, relationships, or personal hobbies,[66] but this knowledge alone does not damage a person's sense of privacy as much as actual observation of how people conduct themselves when they think they are outside of the public eye.[67] Accordingly, arguments that phone metadata should be kept out of the hands of government until it is accessed through properly protected chan-

65. *See* THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECHS., *supra* note 61, at 117 (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

66. *See* Jonathan Mayer, Patrick Mutchler, & John C. Mitchell, *Evaluating the Privacy Properties of Telephone Metadata*, 113.20 PROC. NATL. ACAD. SCI. U.S. 5536 (May 17, 2016), http://www.pnas.org/content/113/20/5536.full [https://perma.cc/NCB8-JA4D]; Bjorn Carey, *Stanford Computer Scientists Show Telephone Metadata Can Reveal Surprisingly Sensitive Personal Information*, STANFORD.EDU (May 16, 2016), http://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/ [https://perma.cc/X5GS-C2CX].

67. *See* Cohen, *supra* note 25 ("The injury . . . does not lie in the exposure of formerly private behaviors to public view, but in the dissolution of the boundaries that insulate different spheres of behavior from one another."). Thus, actual observation is a far more damaging privacy infringement than merely gathering information about the same activities. For instance, many would likely not want the public to see them carrying out even routine activities inside the home, such as sleeping and eating, even though that information is nothing harmful or unusual.

nels should similarly counsel a policy of private control over body camera footage.

Implementing a system of third-party control would be logistically simple. Because police departments employing this technology are already transmitting body camera footage to be stored on remote servers,[68] the only change required to avoid privacy concerns associated with unchecked police control of footage would be for third parties to limit law-enforcement officials' access to these servers. This move mirrors the strategy adopted by the Freedom Act — to leave the data under exclusive control of the private carriers who already collect and manage it.

Transitioning to exclusive third-party storage and control would not necessarily entail a dramatic increase in the cost of administering a body camera system, since many (if not all) currently funded body camera programs already pay for third-party storage.[69] The main difference in cost would be accounting for third-party control over access to and release of body camera footage, as well as the provision of redaction services for accessing footage. The cost of redaction services could be partially offset by charging a reasonable amount to private accessors of footage. Although this system would likely still result in a net cost increase to the government, which would request footage and pay for redaction, the cost increase should not be considered prohibitive to carrying out implementation in the manner most beneficial to the public given the demand for body cameras across the nation and the added protections this recommendation would provide.

C. CRITICISMS OF PRIVATE STORAGE

To be sure, transitioning to complete private storage would present its own obstacles. Private entities may have less accountability or their own incentives to violate the privacy of indi-

68. Martin Kaste, *As Police Body Cameras Increase, What About All That Video?*, NAT'L PUB. RADIO ALL TECH CONSIDERED (May 31, 2015), http://www.npr.org/sections/alltechconsidered/2015/05/29/410572605/as-police-body-cameras-increase-what-about-all-that-video [https://perma.cc/QP36-VPP4]; *see* VIEVU SOFTWARE, http://www.vievu.com/vievu-products/software [https://perma.cc/5HDD-3WHU] (last visited Dec. 30, 2016) (listing plans for upload, storage, and management of evidence, including body camera footage).

69. No examples could be found of police departments that store body camera footage on in-house servers or otherwise entirely within their possession.

viduals on footage. Policymakers must, therefore, consider both the privacy harms presented by private storage in addition to the practical difficulties of implementation.

The recommendation by the President's Review Group to move phone metadata to private hands provides a case study of privacy concerns that should be considered before making a similar change with respect to body camera footage. One national security observer has criticized the recommendation to store phone data with private companies as implicating a wide array of new issues without adequately solving the risk of misuse:

> This strike[s] me as a bad trade purely in civil liberties terms. Instead of having one actor with a metadata database — an actor that is politically accountable and subject to all kinds of oversight mechanisms — we would now have, depending on how one implemented this idea, several different ones, some with commercial interests. We'd have to build new oversight mechanisms from scratch. If we have the individual companies hold their own metadata, that will mean worrying about what commercial uses *they* might make of them, and we will have to create regulatory, enforcement, and oversight mechanisms to guard against abuse on that front. . . . [P]roliferating the number of people and organizations with access to a sensitive database creates proliferating opportunities for abuse by those organizations and people.[70]

In other words, a move to prevent governmental privacy infringements could lead to increased privacy risks in other areas, owing partially to the lack of accountability and oversight of private companies.

These critiques of the Freedom Act recommendation, however, are not nearly as salient in the body camera context. The primary distinction is that private body camera companies already store and manage body camera footage for law-enforcement agencies, so implementing a private-management policy would entail only logistical changes that create virtually no new privacy concerns. Thus, because the group of people who have access to the

70. Benjamin Wittes, *Assessing the Review Group Recommendations: Part II*, LAWFARE (Dec. 26, 2013), https://www.lawfareblog.com/assessing-review-group-recommendations-part-ii [https://perma.cc/5A68-BEKR].

body camera footage remains the same, many of the privacy-privacy tradeoffs from the Freedom Act context simply do not apply. If anything, transitioning to private control would provide significantly more protection than exists currently, as it would require police officers to obtain the footage from another party with its own safeguards.

In addition to the fact that these private companies already house body camera footage, there is much less of a concern that companies in this context would leak footage for commercial purposes as compared to companies storing bulk metadata. Unlike bulk data, which can be useful to those involved in marketing, it is difficult to see how there could be much incentive for private parties to illicitly obtain body camera footage, especially en masse.[71] Although there is still a possibility that footage will be leaked improperly, the danger of improper or undesirable use by law enforcement arguably outweighs this risk. This concern may also be addressed by simply tracking access to footage; since there is essentially no legitimate reason for employees to view or transfer this footage except when access has been requested for an official purpose, tracking access may provide adequate risk of detection, thus deterring illegitimate use. There would be no increase in existing cybersecurity risks, because these manufacturers already house this data (and in fact, as companies that specialize in cloud storage, are likely to be better equipped to protect it than police departments).

Concerns over private storage in this context therefore present no significant new risks given how body camera technology and policy have already adapted toward some form of private storage. Given that private storage finds support in an existing policy recommendation and in fact presents the same, if not fewer, privacy and security risks in the context of body camera footage than in the context in which it was originally recommended, third-party control over footage is not a radical move. Rather, it presents a

71. Though the incentive to use footage for extortion may still exist, the risk is significantly smaller. For one, employees handling the data will have much less knowledge of what footage contains exploitable information on particular individuals, unlike officers, who have firsthand knowledge of encounters and the identities of the subjects. Further, it would be difficult for an employee to illicitly access footage without being detected, due to the aforementioned access logging and lack of legitimate purpose to access footage that has not been requested. These factors do not eliminate this risk, but indicate that it may not be so substantial as to warrant hesitation with increased use of private storage.

rational solution in line with a policy already considered and partially implemented by the federal government in another context.

Critics of third-party control may also argue that the dangers of police-department storage can be more cheaply mitigated solely by implementing better policies for storing and accessing recordings, rather than by transferring these functions to private companies. This is the approach the federal government takes for surveillance conducted under the Foreign Intelligence Surveillance Act.[72] FISA adopts a strategy of "minimization procedures," which it defines as:

> specific procedures . . . reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information . . . .[73]

In other words, FISA minimization procedures are intended to prevent the use of material gathered for a specific purpose (i.e., foreign-intelligence gathering) from being used for ordinary criminal investigations.[74] These procedures include restrictions on the dissemination[75] of information identifying certain individuals, allowing transfer only to certain recipients for purposes relevant to foreign intelligence surveillance goals.[76] The Freedom Act

---

72. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-411, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–11) (2012) [hereinafter "FISA"]; *see also id.* § 1801(h) (defining "minimization procedures").

73. *Id.* § 1801(h)(1).

74. *See In re* Sealed Case, 310 F.3d 717, 721 (FISA Ct. Rev. 2002) ("'[M]inimization procedures' [are] designed to prevent the acquisition, retention, and dissemination within the government of material gathered in an electronic surveillance that is unnecessary to the government's need for foreign intelligence information." (citation omitted)); *Foreign Intelligence Surveillance Act (FISA)*, ELEC. INFO. PRIVACY CTR., https://epic.org/privacy/terrorism/fisa/#Overview [https://perma.cc/4FRU-YJWG] (last visited Mar. 4, 2016) ("Minimization procedures are designed to prevent the broad power of 'foreign intelligence gathering' from being used for routine criminal investigations.").

75. Minimization procedures also govern the retention of data. Retention policies under FISA are briefly discussed *infra* Part IV.B.

76. *See* NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES TO BE USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2007) *available at* https://www.aclu.org/files/

builds on these goals by restricting when and how the government can query databases for communication records.[77] Minimization procedures are not designed to prevent retaining or disseminating already-obtained "information that is evidence of a crime which has been, is being, or is about to be committed . . . ."[78] Rather, these procedures exist specifically to "ensure that criminal investigators [outside of the FISA context] do not use FISA authority for criminal investigations."[79] Because private storage of body camera footage would likewise be used to prevent law enforcement from using body cameras beyond their police-oversight role, similar minimization procedures may seem a less burdensome alternative to completely barring police-department control.

Minimization procedures, however, would not be enough to mitigate the privacy risks inherent in law enforcement's control over recordings. First, minimization procedures have drawn significant criticism as a safeguard against FISA surveillance for being ineffective or easily circumvented.[80] Further, many of the concerns discussed in this Section — including the ability to access or tamper with footage without authorization — do not stem from weak rules, but rather the potential for those in control to break these rules. Because the very fear of such abuse is a privacy harm and members of the public already fear official miscon-

---

natsec/nsa/minimization_procedures_used_by_nsa_in_connection_with_fisa_sect_702.pdf [https://perma.cc/88KW-BXSQ].

77. *See* Amel Ahmed, *Landmark Ruling on NSA Sweep Pushes Case for Stronger Surveillance Reforms*, AL JAZEERA AM. (May 9, 2015), http://america.aljazeera.com/articles/2015/5/9/federal-court-deals-death.html [https://perma.cc/B68M-KYDK] ("Under the [Freedom Act], before the government can access the bulk data, it would need to present to the FISA court a 'specific selection term' that identifies a person, account, address, or any other discrete identifier. 'The addition of the language [means that] there will have to be a nexus between the query and the investigation,' [Elizabeth Goitein, co-director of the Brennan Center for Justice's Liberty and National Security Program] said."); *supra* note 64 and accompanying text.

78. 50 U.S.C. § 1801(h)(3) (2012).

79. ELEC. INFO. PRIVACY CTR., *supra* note 74.

80. *See, e.g.*, Mark Jaycox & Rainey Reitman, *The New USA Freedom Act: A Step in the Right Direction, but More Must Be Done*, ELEC. FRONTIER FOUND. (Apr. 30, 2015), https://www.eff.org/deeplinks/2015/04/new-usa-freedom-act-step-right-direction-more-must-be-done [https://perma.cc/C2CW-XWER] (claiming the Freedom Act did not sufficiently strengthen minimization procedures); Kurt Opsahl & Trevor Timm, *In Depth Review: New NSA Documents Expose How Americans Can Be Spied on Without a Warrant*, ELEC. FRONTIER FOUND. (June 21, 2013), https://www.eff.org/deeplinks/2013/06/depth-review-new-nsa-documents-expose-how-americans-can-be-spied-without-warrant [https://perma.cc/ZQ34-4XBU] (criticizing "various loopholes" and claiming that the NSA "has decided to minimize the minimization").

duct, formal rules without practical barriers may do little to assuage the concerns that footage will be mishandled or used maliciously. Additionally, minimization procedures are not mutually exclusive with a transition to third-party management, so these FISA surveillance policies could certainly inform the rules for private entities once the transition is made. Even if minimization procedures are the best framework for preventing abuse of data held by law-enforcement or government officials, it is no substitute for removing this data from the possession of law enforcement altogether.

A privacy-centric approach thus strongly counsels a transition to third-party management, because the risks are substantially lower than those inherent and inevitable in a system wherein law enforcement controls footage collected to monitor their own encounters with the public. To be sure, there are several practical considerations that must accompany this transition. Those questions must be the focus of the current dialogue. For body cameras to best serve the public, policymakers should use this critical time in which programs are not yet entrenched to focus on how to fund this move to private storage, how to determine precisely who will be entrusted to manage the footage, and how to properly monitor private entities to prevent privacy violations of their own.[81]

Therefore, while exclusive private management of body camera footage presents its own obstacles, this alternative demonstrates the substantial policy differences that can result from more focus on the privacy considerations of body camera implementation. The lack of this perspective in current dialogue has perhaps contributed to the failure to seriously consider management by non-law-enforcement entities, and it is precisely this

81. This Note will not fully explore the details of such policies, but if the transition to privately managed storage does occur, policymakers must thoughtfully account for several risks in advance. For one, they must carefully craft policies to ensure that data is in fact secure from employee leaks and outside access. They must also account for how the private companies themselves will be held accountable (even though this Section suggests that these concerns will be less serious for footage in private hands), without reintroducing the problem of unrestricted government access.

They must also determine several specifics before implementing such a policy. As for the type of company that will manage footage, it may be the case that the manufacturers who now provide an analogous service transition into this more official role for the long term, but it may be more desirable to create new entities aimed specifically at this function. The same provider may carry out storage and redaction, or outsource the latter when footage must be released. These questions are important, but they cannot be properly evaluated until policymakers commit to exclusive private storage as a solution to the privacy flaws of the status quo.

kind of omission from policy considerations that must be remedied by a more-complete assessment of privacy interests. Moving forward, a focus on privacy should counsel more thorough consideration of issues such as who manages and controls access to footage, regardless of whether that framework ultimately leads to a policy akin to the one this Note suggests or an intermediate solution.

IV. CONTROLLING ACCESS

Policies governing who can access footage, in what form, and under what circumstances give rise to one of the most consequential ongoing debates surrounding body camera implementation. Regardless of who controls access to the footage, policies regulating when it can be accessed have enormous implications for how effectively a body camera program can protect privacy interests. Policymakers should thus carefully calculate the privacy harms and benefits accompanying each part of an access policy to ensure that the withholding or release of footage cannot compromise the overarching goals of a body camera program.

A. ISSUES WITH OVERLY OPEN ACCESS POLICIES

Advocates of body cameras often consider public access to footage that may depict law-enforcement misconduct to be an important tenet of access policies.[82] This desire reflects a fear that misconduct will go undiscovered or unpunished if the public is not able to view footage of police interactions with the public. The ACLU, for instance, deems a policy in favor of openness essential to proper police oversight.[83] An increased focus on the

82. *See* MILLER ET AL., *supra* note 49, at v (In an introductory letter to the report, Chuck Wexler, Executive Director of the Police Executive Research Forum, says that "with certain limited exceptions . . . body-worn camera video footage should be made available to the public upon request — not only because the videos are public records but also because doing so enables police departments to demonstrate transparency and openness in their interactions with members of the community."); ACLU Letter to DOJ, *supra* note 15, at 5 ("LAPD's failure to gear its body-worn camera program towards transparency and building public trust is evident in the Department's approach to public access to video footage. . . . [H]igh-ranking members of the Department have repeatedly said that the Department will treat body-worn camera videos as categorically exempt from disclosure under California's public records law . . . .").

83. *See* ACLU RECOMMENDATIONS, *supra* note 4, at 8 ("Flagged recordings are those for which there is the highest likelihood of misconduct, and thus the ones where public oversight is most needed. Redaction of disclosed recordings is preferred, but when that is

privacy aspects of such policies, however, demonstrates that a regime of overly open public access to footage may cause a substantial — and avoidable — negative impact on privacy interests.

The ACLU's recommendations, although thorough and committed to privacy protection, are guided by a strong preference for openness, which leads to a misestimation of net privacy impact in the development of certain policies. The recommendations rely heavily on a "flagging" system, whereby footage more likely to show police abuse is much more easily accessible.[84] Videos can be flagged by the subject of a police encounter or by the police department upon belief that misconduct has occurred, and automatic flagging would occur upon a complaint, any use of force, or any incident that leads to detention or arrest.[85] The ACLU recommends that footage lacking such flagging should be publicly disclosed only with the consent of the subject or if the subject's identity has been redacted.[86] However, fearing that overly restrictive requirements for public release will undermine body cameras' role in enforcing public accountability, the ACLU recommends that "flagged recordings should be publicly discloseable," without regard to subjects' consent and without redaction if infeasible (although redaction is preferred).[87] Thus, under these guidelines, consent would be required for unflagged and unredacted recordings but the flagged recordings would be exempt from the consent requirement, "because in such cases the need for oversight [of law enforcement] generally outweighs the privacy interests at stake."[88]

Policies designed in accordance with these guidelines would underestimate the negative privacy impacts in three key ways. Namely, such policies would overlook the harms of (1) regularly allowing for release of footage against the will of the subject of police encounter, (2) depending too heavily on redaction as a means of eliminating privacy concerns, and (3) remaining overly permissive in allowing government access for investigatory purposes.

---

not feasible, unredacted flagged recordings should be publicly discloseable, because in such cases the need for oversight generally outweighs the privacy interests at stake.").

84. *See id.* at 6.

85. *See id.*

86. *See id.* at 7 (this disclosure would apparently apply without regard to consent).

87. *Id.* at 8.

88. *Id.*

First, unconsented release of footage, even in the name of oversight or transparency, has a significant detrimental privacy impact. The footage itself could harm the subject by revealing personal information, depicting victims of crimes in vulnerable states, or publicizing private activity within a home or other non-public area. Sensitive or incriminating footage may also be used maliciously or coercively by others if the subject's consent is not required. Additionally, there are practical concerns with using flagging as an automatic mechanism to release footage. Flagging occurs, among other instances, when a person files a complaint for police misconduct.[89] If a consequence of filing such a complaint were public disclosure of unredacted footage, victims of potential police misconduct may be deterred from reporting such misconduct, meaning body cameras would no longer provide effective oversight. Individuals who are recorded in particularly vulnerable moments, including those who are victims of law-enforcement abuse, would have to consider whether exposure of this incident to the public would be worth the potential embarrassment that could arise from pursuing a complaint. Once a video is flagged, a subject who did not consent to release would have to simply hope that others do not propagate sensitive and uncensored footage. Even if the mainstream media exercised restraint in showing or revealing private information, total public accessibility could result in anonymous or less-accountable actors releasing complete footage online. The nature of body cameras makes this concern substantially greater than it would be in the case of dashboard cameras, for instance, because dashboard cameras will generally not record encounters in as much detail as body cameras, and they will not record inside areas such as the home.[90] Circumventing the subject's consent as a requirement of releasing footage to the public thus entails significant net privacy costs while doing little to increase accountability.[91]

Second, these access recommendations assume that redaction sufficiently reduces (or even negates) risks to privacy interests. In many instances, this is not the case, and unconsented disclosure is still a serious concern. Redaction is not a binary decision:

---

89. *See id.* at 6.

90. Even for encounters that take place in public outdoor areas, body cameras are much more intrusive to privacy because they record the encounter from much closer perspective with clearer views of the subject.

91. *See infra* Part IV.B (further evaluating redaction as a privacy safeguard).

subjects and locations may be identifiable in a video despite careful efforts to obscure features such as faces, voices, and addresses. For instance, the victim of a serious crime that occurs in his or her own home will be identifiable to family and friends familiar with the inside of the home, regardless of how thoroughly their features are obscured. This presents harms to individuals similar to the harms of unredacted release, including that people who find compromising footage could threaten disclosure for coercive reasons (such as extortion or blackmail). Even if the subject can confidently know that no one will be able to deduce his or her identity from the redacted footage alone, records and officer accounts could still link the subject to the footage. The realistic limitations of redaction not only leave open the possibility of a subject actually being identified in a private and potentially compromising setting, but perhaps more importantly, these shortcomings present a constant fear for people recorded in such circumstances that the footage can be shown without their consent.[92]

Third, such policies would fail to properly limit access by law enforcement and other government officials for purportedly legitimate purposes, such as official investigation or informal review. The ACLU recommendations make little reference to this kind of access, despite the serious concerns implicated in allowing unrestricted access to footage for use in criminal investigations.[93] Such unchecked access heightens the risks of dragnet-style policing by failing to ensure the bar to review footage is sufficiently high to prevent what are essentially fishing expeditions, and it compounds the already-present risks that the footage might be abused by granting access to other agencies (including prosecutors as well as other state and federal agencies).

---

92. *See supra* note 25 (discussing the harms to privacy and autonomy that result from the fear of surveillance).

93. The ACLU states that it is important "to ensure that video is only accessed when permitted according to [these policies], and that rogue copies cannot be made[,]" but there are no recommendations as to official police or government review. ACLU RECOMMENDATIONS, *supra* note 4, at 8. It seems then that the recommendations are concerned only with improper unofficial use, such as "pass[ing] around video of a drunk city council member, or video generated by an officer responding to a call in a topless bar, or video of a citizen providing information on a local street gang." *Id.* While the ACLU did express extreme concern with the LAPD reviewing footage before writing reports, it took no stance against otherwise allowing footage to be used for investigations. *See generally id.*; ACLU Letter to DOJ, *supra* note 15.

These concerns demonstrate the significant risks that accompany even well-intentioned policy regimes that start with a normative focus on openness rather than privacy. To be sure, appropriate access to footage is necessary to effectuate the accountability goals of body cameras as well as the resultant privacy benefits. However, a privacy-focused approach can preserve these accountability objectives while avoiding the pitfalls entailed in a strategy that errs on the side of allowing access.

B. ALTERNATIVE POLICIES SUGGESTED BY A PRIVACY-FOCUSED APPROACH

A privacy-centered analysis demonstrates that alternative policies can adequately serve oversight and accountability interests without causing serious harm to privacy interests risked by excessive openness. There may be policy choices equally or more effective than those discussed in this Note, but the set of alternatives suggested in this Section reveals that privacy interests can be better served without compromising the central purpose of body cameras to provide evidence of and deter official misconduct.

First, a rule requiring the subject's consent prior to releasing footage to the public would substantially mitigate privacy concerns inherent in policies that allow for regular bypassing of consent. A person who has a direct interaction with law enforcement recorded by a body camera should certainly be able to access the footage upon request without requiring a formal complaint or accusation of misconduct. The subject should also be able to authorize public disclosure. The justification for this rule is simply that the accountability function of body cameras is best preserved when complainants of misconduct can freely access footage. Requiring consent allows for body cameras to maintain their accountability function while also dramatically reducing privacy harms associated with releasing recordings. To be sure, these privacy harms may still exist with respect to other parties appearing on footage, and thus redaction measures should be taken to obscure the identities of these third parties. While such a third party's non-consent may present privacy issues, this concession seems necessary: the main subjects of the video, who are most likely to be the target of misconduct and thus most likely to have their privacy interests adversely affected, should be able to override the objection of third parties, since the actual subjects are

most exposed. Third parties should thus not be allowed to bar the use of footage, for this would allow less-affected individuals to unduly impede the several benefits of body cameras.[94] Without the consent of the direct subjects of encounters, however, footage should not be released in light of the detrimental privacy impact it would have. While a flagging system should remain in place to indicate that certain footage might be needed for an investigation and should not be deleted, flagging should not have any effect on the need for consent.

Such a policy would not significantly impede the oversight function of body cameras, as the ACLU and other organizations advocating openness seem to fear. Footage depicting misconduct would only be withheld if the subject was unable or unwilling to consent to release. The former issue could be resolved with an exception: if a subject is unable to consent to release due to incapacitation, death, or legal status (for example, status as a minor), the right to consent to release could be given to any party who would have the right to pursue a civil claim for any police misconduct that may have occurred.[95] Thus, family members could gain access to footage depicting a relative killed by police to review it for misconduct and potentially pursue recourse. When the subject is simply unwilling to consent, that fact should be taken as evidence that the privacy interests for that individual weigh in favor of preventing release. To be sure, there may be merit to a response that the public's interest in increased oversight and accountability (and thus the accompanying privacy benefits) outweighs those individual concerns. However, because the police and the subject are likely to be the only parties who know how sensitive the footage will be in any one case, the individual subject is best positioned to make that assessment.[96] In any event, a

94. A system in which the withholding of consent by a single party could bar access would also present a holdout problem. A secondary subject of a recording that may contain evidence of misconduct can demand some sort of payment or benefit in exchange for consent, knowing that the complainant highly values the footage.

95. Though there may be an argument to extend this right to those with the ability to sue on behalf of a competent subject of a body camera recording (such as an individual to whom the subject has conferred power of attorney), this situation would allow footage to be released over the active objection of the subject, supposedly on his or her behalf. Since such a subject is likely in the best position to assess his or her own privacy interests, inability to consent seems an appropriate requirement for this exception.

96. One alternative may be to allow for third-party review to determine the value of releasing footage over the subject's objection if the value to the public is sufficient. However, this adds a layer of complexity and cost, as well as concern that the footage will trade hands with even more people who may improperly handle it. Perhaps more importantly,

policy requiring consent prior to disclosure seems overwhelmingly consistent with both the oversight objectives of body cameras and the privacy-oriented approach to policymaking.

Second, while redaction should be exercised as an additional safeguard of identities or sensitive information, policies should not rely on redaction as an adequate replacement for consent or other safeguards. Redaction can be a complex issue; though these questions have not yet been explored in detail by body camera advocates, redaction may pose case-specific questions of who manages redaction, when it must occur and how the costs are covered, and how redaction practices should prioritize certain objectives (such as preserving important information that would be obscured by blurring a face, for instance). While these specifics must be carefully and preemptively decided, it must still be recognized that redaction cannot work perfectly in every instance.[97] Although privacy interests of third parties and victims may be served by protecting their identities when another person requests footage, the result will not be uniformly effective. Thus regardless of the particular protocols chosen, redaction should be exercised when possible, but only as an additional safeguard to access restrictions.

Third, limiting release of footage in order to assist in criminal investigations would be reasonable and easily accomplished using existing legal frameworks. To effectively ensure law-enforcement accountability, government officials who have the power to investigate allegations of police abuse should be allowed access for the purpose of investigating reports of misconduct,[98] but this must be on a case-by-case basis to avoid concerns of unlimited access and dragnet tactics. For example, policies should not allow law enforcement to review footage of a subject's home in search of previously-undiscovered criminal activity under the pretense of evaluating police conduct if there is no basis for such review. Members

---

this potential override of the subject's will in any given case largely undermines the goal of the default rule of consent, because the subject may suffer ongoing anxiety about the potential release of the footage even after the incident has occurred and they have refused to consent to the footage's release.

97. *See supra* Part IV.A (discussing some shortcomings of redaction as a means of protecting sensitive information).

98. Though release to law enforcement for a criminal investigation would often be without the consent of the subject(s), this does not present the same issues discussed *supra* Part IV.A. Here, there would be significant safeguards enforced by a court, and these rules are better tailored to releasing footage only when the public interest in the footage is great.

of the department accused of misconduct should not be granted access to pertinent, since the fear of misuse would be particularly high when those accused can access their own evidence (even if the actual risk is small). Furthermore, the access should be well-documented and transparent, and policies should impose restrictions on how these agencies handle or release the footage.[99]

One approach to limiting access by government officials conducting a criminal investigation would be to require a court order. Under this approach, a court should only grant such an order if the government, in a hearing, where the subject has the opportunity to appear, shows that the footage contains evidence material to a criminal investigation, perhaps by a demanding burden of clear and convincing evidence. This would consider the privacy issues at stake and the fact that body cameras are not intended to be tools of evidence collection. Though this high burden of proof may be administratively difficult for the government to meet, it would ideally keep this method of accessing footage reserved to circumstances where it is truly necessary for an important prosecution. The court order should specify what portions of footage are material and should be released, and, as always, the footage should be redacted to reasonably protect the identity of third parties.[100] Such an approach would mirror the Cable Communications Policy Act,[101] which limits government access to certain information held by cable providers by requiring a court order that the government can only obtain by showing clear and convincing evidence of criminal activity and by meeting the evidentiary threshold of materiality.[102] Under the Act, the individual whose records are under request also has the right to appear and contest such a claim.[103]

---

99. Restrictions similar to FISA minimization procedures may be useful in governing how government agencies handle footage. *See supra* Part III.B (discussing FISA minimization procedures for the disclosure of data and the potential place for analogous procedures in managing body camera footage).

100. These identities should be unredacted if the government can show, in the initial or subsequent hearing, either that these identities are material to the investigation or that the footage cannot properly be redacted while still providing the information the government needs. Consider, for example, footage in which the illegal activity can only be shown by revealing the identity of an innocent third party. This may be the case in instances of violent crime.

101. 47 U.S.C. § 551 (2012).

102. *Id.* § 551(h)(2).

103. *Id.*

Body camera footage is likely to be much more sensitive than information held by cable providers. On the other hand, this footage can be extremely probative evidence of criminal activity. Thus, body camera footage should be similarly made accessible upon a showing that law enforcement has a sufficient justification to believe that the footage contains material evidence. Although the Act manages a different type of privacy issue (cable companies are not in the business of collecting data inherently linked to law-enforcement activities), it still provides a useful framework for protecting highly private information that occasionally may be extremely useful for legitimate law-enforcement purposes. The similarity of privacy concerns in the cable context and the body camera context should counsel a similar solution.[104] This requirement of an intermediary's approval before allowing law enforcement to use footage as criminal evidence also finds support in the FISA minimization procedures. One such procedure is an "information screening wall," or the use of an official not involved with the criminal investigation to review evidence and only pass on what is relevant to a previous or impending crime.[105] This high bar would limit fishing for evidence, because it must be shown ex ante that relevant evidence is likely present. In cases in which the requestor can demonstrate an urgent need for footage, these standards could be loosened.[106]

---

104. This difference may support a lower burden of proof than clear and convincing, because the concerns about law enforcement accessing a private company's business data are not present. Regardless of such implementation details, the Act mitigates risks very similar to those present in the context of body camera footage, so the framework remains a persuasive model for a solution.

105. ELEC. INFO. PRIVACY CTR., *supra* note 74. This official is not necessarily a judge in the FISA context. *Id.*

106. Such an extraordinary exception should be limited to circumstances involving time-sensitive information. Such rapid access may not allow time for redaction; thus, an emergency exception should be carefully and narrowly defined. This exception could require, for example, that (1) there is an imminent need to review the footage of a specific incident for purposes of public safety, (2) that need substantially outweighs the aggregate interests of keeping the footage private, and (3) there is no other method by which the information sought can be obtained in a reasonable amount of time given the circumstances. Such restrictions would allow for footage to be accessed in emergency situations but restrain that access to times when the necessity is great and there is no less-harmful alternative.

A properly defined emergency exception could limit the government's ability to use body cameras for evidence collection, because footage so obtained would require truly exigent circumstances that typically could not be foreseen at the time of recording. Such an exception would prevent the withholding of footage that is necessary to prevent an impending criminal act, and therefore may be invoked, for instance, when a person present at a previous crime scene presents a threat to public safety.

This framework is merely one alternative to the current regime, which places little to no barrier to the government's access to body camera footage, so long as there is a claim that it relates to an investigation. A policy similar to this one would not significantly interfere with legitimate government use of footage, but would place powerful privacy safeguards where none currently exist.

These alternatives demonstrate the flaws of an approach to policymaking that does not fully consider the wide array of privacy interests. By failing to account for privacy harms and privacy benefits in various forms, policies may be carefully designed but nevertheless compromise privacy interests with no concomitant benefits in the form of body camera effectiveness. The privacy side of the equation has thus been miscalculated when considering access policies for body camera footage, causing policymakers to miss alternatives that substantially protect and benefit citizens' privacy when they encounter police officers equipped with body cameras. For the technology to most effectively serve these interests, policymakers must reorient their views around privacy.

V. CONCLUSION

Body cameras have demonstrated a great potential to curb police abuse and have generated great public excitement as the technology is used more often. The need for improved law-enforcement accountability and the important privacy interests implicated by more recording of the public both necessitate great care in crafting thoughtful policy as body camera technology becomes more widespread. These policies, however, cannot fully serve the public with the narrow conception of privacy that currently prevails, which assumes that body cameras are strictly detrimental to privacy interests. Instead, the full picture of the privacy impact — including both harms and benefits, even when they take unexpected forms — should be at the core of these policy determinations.

While there will be practical obstacles to implementing these policies and achieving uniformity across states and municipalities, adopting a complete perspective of the privacy interests at stake is a vital first step. By embracing a privacy-focused viewpoint that accounts for both harms and benefits, policymakers can move beyond the framework of strict privacy-accountability

tradeoffs, instead ensuring that body cameras achieve their accountability purpose while best serving the privacy interests of civilians.