VIRGINIA LAW REVIEW ONLINE

VOLUME 105 FEBRUARY 2019 57-66

ESSAY

LAW ENFORCEMENT'S PAIRING OF FACIAL RECOGNITION TECHNOLOGY WITH BODY-WORN CAMERAS ESCALATES PRIVACY CONCERNS

*Katelyn Ringrose**

INTRODUCTION

Half of American adults are currently in a law enforcement facial-recognition network.[1] As the use of body-worn camera ("BWC") technology by law enforcement increases, the demand for facial-recognition technology likewise accelerates.[2] Through grants called Smart Policing Initiatives, the U.S. Department of Justice has dedicated over $20 million to provide BWCs for law enforcement across the nation.[3]

* J.D., Notre Dame Law School, Expected 2019. Katelyn Ringrose writes on issues at the intersection of surveillance and privacy, including facial recognition technologies, genetic testing, and social media. She thanks Professor Patricia L. Bellia, Notre Dame Law School's cyberlaw expert, for her valuable input.

[1] Clare Garvie et al., Geo. L. Ctr. on Privacy & Tech., The Perpetual Line-Up: Unregulated Police Face Recognition in America 1 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [http://perma.cc/G9FK-ACCM].

[2] Id. at 29.

[3] Press Release, U.S. Dep't of Justice, Department of Justice Awards Over $20 Million to Law Enforcement Body-Worn Camera Programs (Sep. 26, 2016), https://www.justice.gov/opa/pr/department-justice-awards-over-20-million-law-enforcement-body-worn-camera-programs [http://perma.cc/P7V5-6WG3]. There have been legal arguments both for and against the widespread use of body cameras. See generally Michael D. White, Police Officer

Companies are racing to integrate BWCs with facial recognition technology, hoping to eventually use artificial intelligence to recognize faces captured in real time, despite privacy concerns.[4] Once equipped with facial-recognition technology, BWCs could dramatically increase the number of individuals logged in law enforcement facial-recognition networks, enabling police officers to act as sophisticated surveillance mechanisms.[5]

Anyone passing a police officer equipped with this technology may be scanned, identified, and cataloged in a facial-recognition database without being suspected of any crime or even communicating with the officer.[6] This transforms walking down a street where police are present into a police interaction.[7] In addition to the very real possibility that bad actors might potentially get a hold of the resulting data, facial-recognition technologies disproportionately affect people of color, and integration with BWCs carries the probability of chilling free speech in public spaces.

Body-Worn Cameras: Assessing the Evidence (2014), http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=492D2B3F28A31AFEDFB411749436AB7F?doi=10.1.1.683.3623&rep=rep1&type=pdf.Although they were implemented following a nationwide push against the shooting of unarmed black men by police and have been widely regarded as a positive adoption when it comes to civilian–police altercations, recent studies have shown that the use of BWCs has not had any dampening effect on police violence. David Yokum, Anita Ravishankar & Alexander Coppock, Evaluating the Effects of Police Body-Worn Cameras (The Lab @ DC, Working Paper, 2017), https://bwc.thelab.dc.gov/TheLabDC_MPD_BWC_Working_Paper_10.20.17.pdf [http://p erma.cc/GN3P-QT8F].

[4] Ava Kofman, Real-time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines, The Intercept (Mar. 22, 2017, 2:23 PM), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/ [http://perma.cc/6Z62-ACCM].

[5] Patrick Tucker, Facial Recognition Coming to Police Body Cameras, Defense One (July 17, 2017), https://www.defenseone.com/technology/2017/07/facial-recognition-coming-police-body-cameras/139472/ [http://perma.cc/QF35-ALKU].

[6] Tom Simonite, Few Rules Govern Police Use of Facial-Recognition Technology, Wired (May 22, 2018, 9:35 PM), https://www.wired.com/story/few-rules-govern-police-use-of-facial-recognition-technology/ [http://perma.cc/8BHJ-4XY3].

[7] Letter from Civil Rights Groups to the Axon AI Ethics Board 1–2 (April 26, 2018), http://civilrightsdocs.info/pdf/policy/letters/2018/Axon AI Ethics Board Letter FINAL.pdf [http://perma.cc/6YJF-36EC]. It has recently been found that several cities used body cameras to gather information on Black Lives Matter protesters in order to create a "watch list." Aris Foley, Memphis Police Store Secret Surveillance of Black Lives Matter Protesters for 'Watch List,' AOL.com. (Feb. 21, 2017, 12:30 PM), https://www.aol.com/article/news/2017/02/21/memphis-police-store-secret-surveillance-black-lives-matter-protesters/21718619/ [http://perma.cc/GW9F-28J2]. In addition to the First Amendment concerns raised by the Black Lives Matter allegations, it is an open question whether law enforcement's ability to image and identify an innocent civilian presents the potential for a Fourth Amendment search.

Although technology often outpaces legislation, privacy law must rise to meet the requirements of the First and Fourth Amendments in response to the integration of facial-recognition technology and BWCs.

In Part I, this essay examines the history of BWCs, contemporary use, and probable future impact. Part II analyzes how their integration with FRT disproportionately impacts African Americans, chills free speech, and implicates privacy concerns.[8] Part III describes how different federal and state courts and legislatures have handled real time data collection through new technologies.[9] This essay concludes with recommendations for lawmakers regarding retention and utilization of camera footage collected via BWCs.

I. PAIRING BWCS WITH FACIAL RECOGNITION TECHNOLOGIES

Increasing public attention on police shootings of unarmed black victims has ignited discussion around BWCs. But the government, the courts, and the public all lack an adequate understanding of the dangers of integrating BWCs with biometric technologies, like facial-recognition technology, and are currently ill-equipped to deal with the resulting, rapidly approaching surveillance state.

In an effort to correct unconstitutional practices and eliminate racial discrimination, a federal district court in New York ordered officers to use BWCs.[10] In *Floyd v. City of New York,* the court identified BWCs as an exceptional way to prevent constitutional harms.[11] First, the court found that BWCs "will provide a contemporaneous, objective record of stops and frisks."[12] These recordings can validate whether a stop and frisk was warranted.[13] Second, the court reasoned that when citizens and police officers know that an exchange is being recorded, this will foster an environment of mutual respect and lawful interactions between the parties.[14] Third, according to the court, BWC recordings will serve as a

[8] Mariko Hirose, Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology, 49 Conn. L. Rev. 1591, 1618–19 (2017).

[9] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that the use of cell site location information by law enforcement constitutes a search in some circumstances).

[10] Floyd v. City of New York, 959 F. Supp. 2d 668, 685 (S.D.N.Y. 2013).

[11] Id.

[12] Id.

[13] Id. (footnote omitted).

[14] Id.

legitimizing measure in response to police distrust, particularly in communities where stops and frisks are disproportionately directed.[15]

But law enforcement agencies like the New York Police Department are not motivated solely by protecting constitutional rights and incentivizing good behavior, as their zeal for pairing facial recognition technology with BWCs makes apparent.[16] It is expected that the use and adoption of BWCs will continue to accelerate, and the FBI has stated that adopting greater facial-recognition technologies is central to its mission.[17] But the FBI also realizes that this evolving technology will require clear policies and regulations.[18]

Given the push for law enforcement agencies to adopt innovative surveillance technologies as quickly as possible,[19] development of facial-recognition technology that will pair with BWCs is quickly gaining market importance.[20] A 2016 U.S. Department of Justice–funded study found that at least nine out of thirty-eight BWC manufacturers currently include some form of facial recognition in their camera technology or are planning for its possible future inclusion.[21]

[15] Id. The court also noted the benefit to officers who would be required to wear the camera. Id. ("Video recordings will be equally helpful to members of the NYPD who are wrongly accused of inappropriate behavior.").

[16] See generally Fanny Coudert et al., Body-worn Cameras for Police Accountability: Opportunities and Risks, 31 Computer L. & Sec. Rev. 749 (2015) (providing an overview around the goals of BWCs and the risks they may present going forward).

[17] Statement Before the House Committee on Oversight and Government Reform, Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services Division of the Federal Bureau of Investigations, Law Enforcement's Use of Facial Recognition Technology (Mar. 22 2017), https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology [http://perma.cc/6JRD-AYXE] ("[W]e at the FBI cannot fail to meet our assigned mission. We must continue to exceed expectations and never rest on past successes. Hence, we must embrace new technologies such as automated FR and optimize allocated resources to achieve mission objectives.").

[18] Vivian Hung et al., The Johns Hopkins University Applied Physics Laboratory, A Market Survey on Body Worn Camera Technologies 404 (2016), https://www.ncjrs.gov/pdffiles1/nij/grants/250381.pdf [http://perma.cc/5Y7F-K8X4].

[19] Jennifer Lynch, Electronic Frontier Foundation, Face Off: Law Enforcement Use of Face Recognition Technology 1 (2018), https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf [http://perma.cc/6S86-G3BW].

[20] Felix Juefei-Xu et al., A Preliminary Investigation on the Sensitivity of COTS Face Recognition Systems to Forensic Analyst-style Face Processing for Occlusions 25 (Conference on Computer Vision and Pattern Recognition Workshop Paper, 2015), http://xujuefei.com/felix_cvpr15_cots.pdf [http://perma.cc/WCF9-HES3].

[21] Lynch, supra note 19, at 21.

In May of 2018, one of the largest BWC marketers, Axon,[22] gained a patent for software that can find faces and other objects in footage from body cameras in real time.[23] According to the company's patent, "once a face is captured by a user's body-worn camera, a hand-held device 'provides the name of the person to the user of the capture system.'"[24] The development of such a system brings questions about misuse and the potential for arbitrary and reckless application of the technology. In response to those concerns, Axon's CEO said

> there are police forces around the world that use batons and guns in very abusive ways . . . it's too blunt to say that because there is a risk of misuse, we should just write them off. We need to dig a layer deeper and understand what are the benefits and what are the risks.[25]

But who bears responsibility for performing that calculus? Government and law enforcement may lack the inclination to rigorously examine how pairing these technologies may present hidden dangers.

II. RAMIFICATIONS OF INTEGRATION

Many government agencies encourage the use of facial-recognition software with BWC-accrued footage.[26] The Department of Justice focuses on the practical benefits of receiving identification in real time and the cost savings that agencies will realize by not having to hire and train personnel to review video footage later.[27] But notwithstanding the positive aspects of melding BWCs with facial-recognition technology,

[22] Taylor Soper, Police Body Cam Maker Axon Buys Vievu, Ending Competition Between Rivals, GeekWire (May 4, 2018, 10:21 AM), https://www.geekwire.com/2018/police-body-cam-maker-axon-buys-vievu-ending-competition-rivals [http://perma.cc/BK35-R62W] (citing Joshua Brustein, The Biggest Police Cam Company Is Buying Its Main Competitor, Bloomberg (May 4, 2018, 10:00 AM), https://www.bloom berg.com/news/artic les/2018-05-04/the-biggest-police-body-cam-company-is-buying-its-main-competitor [http://perma.cc/-C2TL-JXPE]).

[23] Alex Pasternack, Cop Cameras Can Track You in Real-Time and There's No Stopping Them, FastCompany, (July 31, 2018), https://www.fastcompany.com/40564084/cop-cameras-can-track-you-in-real-time-and-theres-no-stopping-them [http://perma.cc/BZW2-S7ZS].

[24] Id.

[25] Ian Wren & Scott Simon, Body Camera Maker Weighs Adding Facial Recognition Technology, NPR (May 12, 2018, 8:07AM), https://www.npr.org/2018/05/12/61032088/what-artificial-intelligence-can-do-for-local-cops [http://perma.cc/5EWD-AEVQ].

[26] Kelly Blount, Body Worn Cameras With Facial Recognition Technology: When it Constitutes a Search, 3 Crim. L. Prac. 61, 63 (2017).

[27] Hung et al., supra note 18, at 403.

numerous negative effects require the law's attention before the technology runs rampant. Those effects include, but are not limited to, disparities in how the technology treats African Americans, chilling free speech, and vulnerability to third-party hacking and misuse of data.

It is important to understand who these paired technologies are most likely to impact, and how their technological shortcomings might exacerbate that differential treatment. For example, FRT has far higher error rates when utilized to identify African American faces.[28] Algorithms used in new technology may appear unbiased at first, but according to researchers,

> [t]he deeper we dig, the more remnants of bias we will find in our technology. We cannot afford to look away this time, because the stakes are simply too high. We risk losing the gains made with the civil rights movement and women's movement under the false assumption of machine neutrality.[29]

These automated systems reflect the priorities, preferences, and prejudices of their coders, and this "coded gaze" leads to tangible negative effects for African Americans.[30] Technology so prone to error should not constitute reliable or admissible evidence.

Pervasive government surveillance can also have a chilling effect on freedom of speech. This monitoring demonstrably lessens Americans' "willingness to engage in public debate and to associate with others whose values, religion, or political views may be considered different from their own," leading to a "spiral of silence."[31] Anonymous free speech is

[28] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proc. of Machine Learning Res. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [http://perma.cc/HRR9-69HX] (scrutinizing algorithmic bias in FRT from Microsoft, IBM and Face++ Cognitive Services showing significant differences in average error rates between light-skinned men and dark-skinned women).

[29] Overview of Gender Shades Project, MIT Media Lab, Massachusetts Institute of Technology School of Architecture + Planning, https://www.media.mit.edu/projects/gender-shades/overview/ [http://perma.cc/AFB3-GHVF] (last visited Nov. 18, 2018).

[30] Id.

[31] Lynch, supra note 19, at 9. (describing the spiral as "the significant chilling effect on an individual's willingness to publicly disclose political views when they believe their views differ from the majority"). The EFF points to evidence accrued from a social-media experiment, when in 2016, research documented the silencing effect on participants' dissenting opinions when they knew of government surveillance—participants were much less likely to express negative views of government surveillance on Facebook when they perceived that those views were "outside the norm." Id.

protected by the First Amendment,[32] but real-time face recognition will redefine public spaces by destroying anonymity. Anonymous speech allows for the proliferation and protection of views that might be critical of law enforcement. Dissenters might be subjected to negative repercussions if they can be easily identified through the use of facial-recognition technology. And, based on current technology, over time these burdens would disproportionately fall on minorities.

Moreover, a regulatory void in this area prevents state and federal lawmakers from addressing hard questions about security and privacy as related to footage accrued via BWC. BWC data's off-site aggregation increases the risk that bad actors can hijack facial-recognition feeds. Moving data off-site makes it more difficult to ensure that best technical practices are followed.[33] New regulations must protect the staggering amount of third-party biometric data, the collection of which creates tremendous security risk, in addition to profound privacy and civil-liberties problems.[34]

III. CONTEMPORARY CASES AND LEGISLATION SET A LEGAL FRAMEWORK

Select jurisdictions do regulate facial recognition technologies in conjunction with BWCs, but there is no current federal legislative consensus on the matter. In 2015, Oregon passed a law barring facial-recognition searches of recordings from BWCs. That law only touches on recordings, and does not govern the use of real-time footage.[35] Recently, New Hampshire passed a similar law.[36] On a local level, the City of Cincinnati as well as six police departments have adopted similar regulations.[37] Despite this anecdotal progress, there should be a federal

[32] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) ("Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society." (citation omitted)).

[33] Lynch, supra note 19, at 21.

[34] Garvie et al., supra note 1, at 1.

[35] Or. Rev. Stat. § 133.741(1)(b)(D) (2015).

[36] N.H. Rev. Stat. Ann. § 105-D:2(XII) (2017).

[37] Cincinnati Police Dep't, Procedure 12.540, Body Worn Camera System (2016), https://www.cincinnati-oh.gov/police/assets/File/Procedures/12540.pdf [http://perma.cc/4N-NA-8LAX]; see Garvie et al., supra note 1 (providing background data on state and city policies related to BWCs and facial-recognition technology).

consensus on how to best balance technology adoption with privacy, free speech, and security.[38]

The Supreme Court has held that "innocent citizens should not suffer the shock, fright or embarrassment attendant upon an unannounced police intrusion."[39] In 1968, following *Katz v. United States*[40] and *Berger v. New York*,[41] the federal government enacted the Wiretap Act.[42] Since then, law enforcement's ability to wiretap a suspect's phone or electronic device has been constrained primarily by statute, as opposed to constitutional case law.

Case law inevitably has blind spots. *United States v. Carpenter* created a legal loophole through which law enforcement can hold personally identifiable information until it becomes historical, and thereby usable without the need for a warrant.[43] That amount of time is, as of now, undecided. Using the Wiretap Act and the *Katz* concurrence as a possible framework for reform, an individual may enjoy a reasonable expectation of privacy in his image as captured by facial-recognition technology. But once law enforcement's use of facial-recognition technology becomes ubiquitous, surveillance subjects will have more difficulty arguing that the Fourth Amendment protects their image. Thus, arguments arising out of privacy concerns are time-bound.

Regulating law enforcement surveillance via statute is the best way to create a holistic scheme. Legislatures are better positioned than courts to research the complex effects of new technology and to draft legislation accordingly. While drafting, they can benefit from model legislation and

[38] Cf. Rachel Levinson-Waldman, Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public, 66 Emory L.J. 526, 530 (2016) (advocating for a judicial, rather than legislative, consensus by articulating a six-part framework to guide Fourth Amendment analysis).

[39] Ker v. California, 374 U.S. 23, 57 (1963) (Brennan, J., concurring in part and dissenting in part) (footnote omitted).

[40] 389 U.S. 347 (1967).

[41] 388 U.S. 41 (1967).

[42] 18 U.S.C. § 2511 (2012). The Wiretap Act, officially Title III of the Omnibus Crime Control and Safe Streets Act, attempted to codify the Fourth Amendment principles set forth by *Katz v. United States*, 389 U.S. 347 (1967). Current model legislation regarding facial-recognition technology seeks to impose annual reporting of facial-recognition technology used by law enforcement agencies, similar to analogous requirements under the Wiretap Act. Garvie et al., supra note 1, at 102–15.

[43] Jake Laperruque, Privacy After Carpenter: We Need Warrants for Real-Time Tracking and "Electronic Exhaustion," POGO (Jul. 2, 2018), https://www.pogo.org/analysis/2018/07/privacy-after-carpenter-we-need-warrants-for-real-time-tracking-and-electronic-exhaustion/ [http://perma.cc/VSSF-6U2L].

existing biometrics laws governing commercial entities. In the meantime, the public relies on courts to protect civil liberties. When judges are given the task of governing technological innovation, they are often ill-suited to appropriately identify future risks. And jurisdiction-specific case law cannot generate a unified solution to the emerging privacy issues that law enforcement's use of real-time facial-recognition technology on accrued BWC footage raises. Without any federal laws or decisions on the books, this practice will be largely unregulated, aside from any best practices adopted by various agencies in what might be an ad hoc manner.

In addition to the Wiretap Act, legislators may also examine the Video Privacy Protection Act ("VPPA") as well as the Family Educational Rights and Privacy Act ("FERPA") to help formulate model legislation.[44] VPPA and FERPA, although old and limited in scope, provide research-backed definitions of personally identifiable information and regulate how such information should be kept, aggregated and disseminated.[45] For example, FERPA requires that personal information be shared only under specified circumstances.[46] For biometric information, this could mean compartmentalizing data into two or more different sets, with strict limits on who holds the keys connecting them. For facial-recognition technology, this would disaggregate the information that, when combined, most individuals consider private. Those separated data identifiers can include faces along with names, booking numbers, and Social Security numbers. Although compartmentalization is only a small step towards protecting data, it constitutes a massive hindrance for bad actors.

Rather than reinventing the wheel, model legislation on facial-recognition technology recently penned by the Georgetown Law School's Privacy and Technology Center may also be broadened to include provisions directly related to the wearing of body cameras by law enforcement.[47] The model legislation includes recommendations on both the state and federal levels, and addresses many of the concerns raised in this article as to who has access to FRT data, how individuals can go about

[44] Video Privacy Protection Act, 18 U.S.C. § 2710 (2012); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2012).

[45] See 18 U.S.C. § 2710(a)(3), (d); 20 U.S.C. § 1232g(b)(1)(K)(i)– (ii).

[46] Joel Reidenberg et al., Fordham L. Sch. Ctr. on Law & Info. Pol'y, Privacy and Cloud Computing in Public Schools 4–6 (2013), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip [http://perma.cc/7HBG-H9S6].

[47] Garvie et al., supra note 1, at 102–15.

having their data technically forgotten, and proper means of training law enforcement officers. However, the legislation does not ponder the true depth of information that will be gleaned via BWC, and it completely discounts the concept of nonconsensual facial-recognition technlogy. If BWCs are running facial recognition in real time, nonconsensual collection of facial feature data will be collected and retained. While there is little question of facial-recognition technology being utilized in situations where felonies are occurring, BWC manufacturers will push law enforcement to engage facial-recognition technology capabilities at most, if not all, times. Therefore, regulations concerning retention and data aggregation are key. In addition to these concerns, facial-recognition technology's current margin of error when identifying persons of color could lead to disproportionate effects when deployed on BWCs. Proposed legislation should fix this technical issue, while also working to better the technology and alerting law enforcement of efficacy requirements.

CONCLUSION

In order to best limit privacy concerns, the chilling of speech in public arenas, and current technology's discriminatory effects, lawmakers should keep in mind the following five principles: (1) limit the facial-recognition data collected from BWCs; (2) provide notice to communities subject to law enforcement facial-recognition data collection; (3) limit the retention of footage gathered via BWC; (4) strictly limit whom the data may be shared with and for what purposes; and (5) establish independent oversight ensuring police accountability and mitigation of facial-recognition misidentification errors likely to have a racially disparate impact.

It is time for the law to address the critical gaps in democratic and constitutional protections that BWCs and facial-recognition technology create. There needs to be a national consensus on the retention and utilization of real-time camera footage accrued by BWCs. At the very least, cities and states should begin regulating law enforcement's use of facial-recognition software as BWCs become more ubiquitous. More generally, lawmakers must address the various dangers technological integration presents before we unwittingly become a surveillance state.