

# STATEMENT OF

### ALBERT FOX CAHN, ESQ.

# **EXECUTIVE DIRECTOR**

# SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, INC.

# **BEFORE THE**

# COMMITTEE ON PUBLIC SAFETY

# NEW YORK CITY COUNCIL

# FOR A HEARING CONCERNING,

# NYPD'S ROLL OUT OF BODY-WORN CAMERAS

&

INTRODUCTION 1136-2018

# SUBMITTED

November 18, 2019

My name is Albert Fox Cahn, and I serve as Executive Director of the Surveillance Technology Oversight Project ("S.T.O.P.") at the Urban Justice Center. S.T.O.P. advocates and litigates for New Yorker's privacy rights, fighting discriminatory surveillance. I commend Chair Richards for today's hearing, Public Advocate Williams for sponsoring Intro 1136, and I am grateful for the opportunity to discuss the privacy implications of NYPD's body-worn cameras ("bodycams").

I speak today in support of Intro 1136, but I also note that this legislation is just a first step in the fight to ensure that bodycams are a tool of police accountability, and not just another form of public surveillance. I believe further reforms will be needed from the Council, lawmakers in Albany, and the NYPD itself.

### I. The False Promise of Bodycams

Let me be frank, the public has been sold a bill of goods on bodycams. We were promised an increased accountability and justice, but instead we provided police with yet another tool of mass surveillance.

Bodycam adoption was initially driven by police use of force, particularly the 2014 police killings of Eric Garner, Michael Brown, Tamir Rice and many others. Initial evaluations offered the tantalizing promise that bodycams could increase "officer professionalism, helping agencies evaluate and improve officer performance, and allowing agencies to identify and correct larger structural problems within the department."<sup>1</sup> Mayor de Blasio cited these justifications when expanding the NYPD bodycam program, promising to make New York City "fairer, faster and grow trust between police and communities."<sup>2</sup>

The practice has fallen short of this promise, as lax departmental policies allow NYPD officers untenable discretion over when and what to record.<sup>3</sup> At the same time, department officials have exercised their own discretion to shield officers from unfavorable footage, while quickly releasing videos that support their narrative. The net result are cameras that are less a tool to restrain cops and more a facet of public surveillance.

The public privacy impact is exacerbated by the NYPD's growing use of facial recognition and other forms of biometric surveillance. These technologies allow the police to turn a walk down the block into a warrantless search of thousands of New Yorkers.<sup>4</sup> The thought is disturbing, but it is even more alarming when one contemplates the use of such technology near political protests, health care facilities, an alcoholics anonymous meeting, or anyplace else where New Yorkers have heightened privacy concerns.

<sup>&</sup>lt;sup>1</sup> See Cmty. Oriented Policing Servs. & Police Exec. Research Forum, Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned 5 (2014), <u>https://www.justice.gov/iso/opa/resources/472014912134715246869.pdf</u>. <sup>2</sup> Thomas Tracy, De Blasio Pushing for Every Cop, Detective on Patrol to Wear a Body Camera by Year's End, N.Y. Daily News (hep. 30, 2018, 7:53 PN), where a value of the provided provided to the provided pr

<sup>(</sup>Jan. 30, 2018, 7:53 PM), <u>www.nydailynews.com/new-york/de-blasio-wear-body-camera-year-article-1.3788661</u>. <sup>3</sup> *Body-Worn Cameras*, Elec. Frontier Found., <u>www.eff.org/pages/body-worn-cameras</u> (last updated Oct. 18, 2017).

<sup>&</sup>lt;sup>4</sup> Mark Blunden, *Police Bodycams with Facial Recognition to Pick Out Criminals from the Crowd*, Evening Standard (June 24, 2019. 8:54 AM), <u>www.standard.co.uk/news/uk/bodyworn-cctv-cameras-to-pick-out-criminals-from-the-crowd-a4174061.html</u>.

### II. The Need for Greater Statutory Oversight on the Release of Bodycam Footage

Last month, after years of delay, the NYPD released its critical incidents response policy.<sup>5</sup> The twopage order, which is supposed to reassure the public about how footage will be released in the most high-profile cases, lists more than a dozen considerations for whether videos should be made public. Sadly, the order provides discretion in lieu of certainty. Worst of all, the discretion is invested in an individual with a clear conflict of interest: the police commissioner himself. If bodycams are to hold the NYPD accountable, it cannot be the police who choose when images are released. The incentive to hide bad data and show favorable footage will always be too powerful.

Alarmingly, the sole bright-line protection in the entire policy will only benefit the Department. It requires the NYPD to not disclose bodycam video while a use of force investigation is ongoing. Under these directives, when a member of the public is accused of a crime, it's fine to share their video, but when an officer is accused of beating a bystander, suddenly it's unfair to share the video while their disciplinary case is ongoing.

Sadly, the department's track record with prior bodycam policies further undercuts public confidence. Earlier this year, the Civilian Complaint Review Board said approximately 40% of requests<sup>6</sup> for bodycam video were unfulfilled. Alarmingly, in more than 100 cases, the NYPD falsely claimed there was no video when there actually was footage.<sup>7</sup> In additional, the NYPD has repeatedly been denounced by advocates for failing to abide by existing disclosure requirements, such as those under New York's Freedom of Information Law and criminal and civil discovery.<sup>8</sup>

More alarmingly still, NYPD officials have repeatedly defended the use of facial recognition in conjunction with bodycams. Earlier this year, former NYPD Commissioner James O'Neill justified this Orwellian practice with the canard that "facial recognition technology is used as a limited and preliminary step in an investigation."<sup>9</sup> Sadly, this description of facial recognition bears little resemblance to NYPD realities. Officers have been documented texting a "match" to a witness and asking, "Is this the guy?"<sup>10</sup> This leading use of facial recognition can easily contaminate eyewitness memory, leading to misidentification and even wrongful conviction.<sup>11</sup>

https://brooklyneagle.com/wp-content/uploads/2019/07/20190710\_boardmtg\_BWC\_memo-2-1.pdf.

<sup>&</sup>lt;sup>5</sup> N.Y. Police Dep't Operations Order No. 46, Public Release of Body-Worn Camera (BWC) Footage of Critical Incidents (Oct. 18, 2019), <u>https://www1.nyc.gov/assets/nypd/downloads/pdf/public\_information/oo-46-19-bodyworn-camera-footage.pdf</u>.

<sup>&</sup>lt;sup>6</sup> Jeffrey Harrell, *Body Cam Backlog: NYPD Lags on Making Footage Public, Report Finds*, Brooklyn Daily Eagle (July 12, 2019), <u>https://brooklyneagle.com/articles/2019/07/12/body-cam-backlog-nypd-lags-on-making-footage-public-report-finds</u>.

<sup>&</sup>lt;sup>7</sup> Memorandum from Olas Carayannis, Dir. of Quality Assurance and Improvement, Civilian Complaint Review Bd., to Members of the Civilian Complaint Review Bd. 2 (July 5, 2019),

<sup>&</sup>lt;sup>8</sup> Tim Cushing, NYPD Finally Comes Up With A Body Camera Policy, And It's Terrible, Tech Dirt (Apr. 19, 2017), https://www.techdirt.com/articles/a20170416/14021937162/nypd-finally-comes-up-with-body-camera-policy-terrible.shtml

<sup>&</sup>lt;sup>9</sup> James O'Neill, Opinion, *How Facial Recognition Makes You Safer*, N.Y. Times (June 9, 2019), www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html.

<sup>&</sup>lt;sup>10</sup> Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Georgetown Law Ctr. On Privacy & Tech., (May 16, 2019), <u>https://www.flawedfacedata.com</u>.

<sup>&</sup>lt;sup>11</sup> False Testimony/Confessions, Cal. Innocence Project, <u>https://californiainnocenceproject.org/issues-we-face/false-confessions</u> (last visited Nov. 15, 2019).

Each of these problems have their own solutions. For bodycams that means new privacy safeguards and limits on officer discretion when to record. And for facial recognition, it means a moratorium or permanent ban. Following the lead of California, which recently passed a statewide ban on bodycam facial recognition,<sup>12</sup> state Sen. Brad Hoylman recently authored a measure that would go even further for New York's police bodycams.<sup>13</sup>

Intro 1136 will require the NYPD to produce much of the data that reformers and academics need to scrutinize the existing bodycam policies and practices. While transparency is important, it is far from a complete solution. It will be incumbent on lawmakers to then respond to this data and implement the safeguards needed to ensure that NYPD bodycams truly protect the public.

# III. The Persistent Call for Police Accountability

As flawed as the NYPD's bodycam policies may be, it is also clear that the public has profound discomfort at the thought of eliminating, or even curtailing, bodycam adoption. Just over a week ago, hundreds of protesters took to the streets in opposition to the hiring of 500 new MTA officers to target fare evasion. I join these advocates in opposing the additional officers, but I fear that MTA bodycams would not be the remedy these protesters hope.

Even if each and every one of those MTA officers had a bodycam, it would still raise the exact same questions we see with the NYPD: who controls the footage? Until we have a clear answer, there is simply no way to know if these cameras will be a tool of police accountability or the latest form of mass surveillance. Fears of public spying are rooted in our understanding of existing NYPD and MTA surveillance practices.

Just as importantly, they are rooted in an understanding of what information we don't have. The lack of public information on police surveillance is why for more than two years, I've fought for enactment of the only bill to comprehensively regulate NYPD surveillance regime: The Public Oversight of Surveillance Technology ("POST") Act.<sup>14</sup> Beyond expanding use of bodycams, the NYPD has already secured an arsenal of invasive spy tools on the public's dime while thwarting any public disclosure or debate. These tools include items like facial recognition, x-ray vans, and automated license plate readers that can monitor a vehicle's location throughout the city. Facial recognition alone has led to the arrests of thousands of New Yorkers, many wrongly accused of crimes they didn't commit.

These tools pose a privacy threat to all of us, but they pose a particularly potent threat to members of our immigrant communities. All too often, these systems create a risk of information-sharing with federal agencies, including ICE. For example, the NYPD for years has contracted with the private firm Vigilant Solutions, which operates a nationwide database of over two billion license-plate data points.<sup>15</sup> Shockingly, in 2016 we learned that Vigilant Solutions was not just contracting with local

<sup>&</sup>lt;sup>12</sup> Albert Fox Cahn, *Police Bodycams Shouldn't Surveil the People They're Supposed to Protect*, Daily Beast, (Oct. 17, 2019, 5:45 AM), <u>http://www.thedailybeast.com/facial-recognition-tech-is-a-blatant-misuse-of-police-bodycams</u>.

<sup>&</sup>lt;sup>13</sup> S.B. S6776, 242d Leg., Reg. Sess. (N.Y. 2019), <u>https://www.nysenate.gov/legislation/bills/2019/s6776</u>.

<sup>&</sup>lt;sup>14</sup> Public Oversight of Surveillance Technology (POST) Act, N.Y.C. Council Bill Int 0487-2018.

<sup>&</sup>lt;sup>15</sup> See Rocco Parascondola, *Exclusive: NYPD Will Be Able to Track Fugitives Who Drive Past License Plate Readers Across the U.S.*, N.Y. Daily News (Mar. 2, 2015), <u>https://www.nydailynews.com/new-york/nypd-track-fugitivesdrive-license-plate-readersarticle-1.2133879</u>.

police departments, but also with ICE.<sup>16</sup> Perhaps most disturbingly, the NYPD relies on Vigilant Solution's artificial intelligence to map out social networks, label New Yorkers as "criminal associates," and create databases based on the company's unproven algorithms.<sup>17</sup>

The POST Act is not just a comprehensive response, but also a modest one. The NYPD can continue using these tools—no matter how problematic—by complying with limited protections against waste, discrimination, and misuse. In fact, the POST Act would be one of the weakest surveillance reform bills in the country,<sup>18</sup> especially when viewed in comparison to San Francisco's<sup>19</sup> and Oakland's outright bans on facial recognition technology<sup>20</sup> and Massachusetts's proposed state-wide moratorium.<sup>21</sup>

The evidence is clear: civilian oversight of surveillance enhances the public's trust in police departments and is absolutely necessary for public safety.<sup>22</sup> Now, with twenty-nine city council members and the Public Advocate signed on as POST Act cosponsors, the time is long overdue for a hearing before the public safety committee and a vote of the full council. I hope that New York City rises to this challenge before it is too late. We urge the Council to build on the momentum it generates securing a hearing on the POST Act before the end of the year.

<sup>19</sup> See Kate Conger et al., San Francisco Bans Facial Recognition Technology, N.Y. Times (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

<sup>&</sup>lt;sup>16</sup> The Domain Awareness System collects the license plate data scanned by the approximately 500 license plate readers operated by the NYPD and combines it with footage from cameras and other surveillance devices around the city. The NYPD holds on to the license plate data for at least five years regardless of whether a car triggers any suspicion. *See* Mariko Hirose, *Documents Uncover NYPD's Vast License Plate Reader Database*, ACLU (Jan. 25, 2016, 10:30 AM), https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database.

<sup>&</sup>lt;sup>17</sup> See id.

<sup>&</sup>lt;sup>18</sup> See Community Control Over Police Surveillance, ACLU, <u>https://www.aclu.org/issues/privacy-technology/surveillance</u>, technologies/community-control-over-police-surveillance (last visited Nov. 15, 2019).

<sup>&</sup>lt;sup>20</sup> See Opinion, San Francisco Banned Facial Recognition. New York Isn't Even Close., N.Y. Times (May 18, 2019), <u>https://www.nytimes.com/2019/05/18/opinion/nypd-post-act-surveillance.html</u>.

<sup>&</sup>lt;sup>21</sup> See S.B. 1385, 191st Gen. Court, Reg. Sess., (Mass. 2019), <u>https://malegislature.gov/Bills/191/S1385</u>.

<sup>&</sup>lt;sup>22</sup> Oakland, California, and Seattle, Washington, have enacted similar police oversight laws without deteriorating public safety. *See* Opinion, *supra* note 20.