

January 31, 2020

Committee on Judiciary and Public Safety
Council of the District of Columbia
John Wilson Building
1350 Pennsylvania Avenue, NW, Washington, D.C. 20004
Sent via email: callen@dccouncil.us

Dear Chairman Allen,

The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Liberty and National Security Program seeks to ensure that the country's national security laws and policies remain equal to the task of protecting individual rights, constitutional values, and the rule of law. The Brennan Center has worked extensively on the deployment of surveillance technology by law enforcement agencies, publishing reports on issues including predictive policing, social media monitoring, cell phone surveillance, local police involvement in counterterrorism efforts, and more.¹ As part of that work, we support efforts to implement greater transparency and oversight of the MPD's surveillance tools.

Currently, the acquisition and deployment of surveillance technologies by MPD and other local government agencies costs District taxpayers millions of dollars each year and occurs with insufficient public accountability or oversight.² While emerging technologies bring opportunities for officers to do their jobs more efficiently, they also raise issues ranging from ineffectiveness to hidden biases to the potential for misuse. Without

¹ See, e.g., Rachel Levinson-Waldman, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, 61 How. L.J. 523 (2018); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527 (2017); Angel Diaz, *New York City Police Department Surveillance Technology*, BRENNAN CTR. FOR JUSTICE (Oct. 7, 2019), <https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology>; Rachel Levinson-Waldman, *Cellphones, Law Enforcement, and the Right to Privacy*, BRENNAN CTR. FOR JUSTICE (Dec. 20, 2018), https://www.brennancenter.org/sites/default/files/2019-08/Report_Cell_Surveillance_Privacy.pdf; Rachel Levinson-Waldman & Erica Posey, *Predictive Policing Goes to Court*, BRENNAN CTR. FOR JUSTICE (Sept. 5, 2017), <https://www.brennancenter.org/our-work/analysis-opinion/predictive-policing-goes-court>; Faiza Patel et al., *Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security*, BRENNAN CTR. FOR JUSTICE (May 22, 2019), https://www.brennancenter.org/sites/default/files/2019-08/Report_Social_Media_Monitoring.pdf; Michael Price, *National Security and Local Police*, BRENNAN CTR. FOR JUSTICE (2013), https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf.

² See, e.g., *Mayor Bowser Announces \$5 Million Investment to Expand MPD Crime Camera Network*, DC.GOV. (Nov. 25, 2019), <https://dc.gov/release/mayor-bowser-announces-5-million-investment-expand-mpd-crime-camera-network>.

effective oversight, modern surveillance poses serious risks for the civil rights and liberties of the whole community, particularly those most often affected by policing: Black and Brown, Muslim, immigrant, LGBTQ+, and low-income communities, as well as activist groups that often hail from the same communities.

It is time for the District to follow in the footsteps of over a dozen other jurisdictions and adopt a framework that protects the rights of District residents and ensures public oversight of surveillance.³ As a first step, we ask that the Council hold a public roundtable on the state of surveillance in the District. A roundtable would allow District leaders to hear directly from impacted D.C. residents, as well as from privacy and technology experts, about the risks and consequences of unchecked government surveillance – both intended and unintended – and inform a path forward.

As you are aware, a coalition of local and national groups and activists, organized under the banner Community Oversight of Surveillance in D.C., is working on legislation that would require the MPD, as well as any other D.C. entity, to obtain D.C. Council approval prior to acquiring new surveillance technology, subsequent to a mandatory public hearing allowing the public a fair opportunity to provide input.⁴ Under this proposed framework, an entity seeking to acquire surveillance technology would be required to produce a Surveillance Impact Report and Surveillance Use Policy detailing the purpose, location, cost, security, and oversight mechanisms associated with the technology, for review and approval by the D.C. Council.⁵ A Privacy Advisory Committee, to be appointed by the Mayor and D.C. Council, would advise agencies and Councilmembers on the impact of the surveillance technology on civil rights and liberties, and the impacts and risks to vulnerable communities. Finally, the bill would establish periodic auditing and annual reporting to ensure that surveillance technologies continue to contribute to public safety, safeguard privacy, and do not result in a disparate impact on marginalized communities.

This bill does not seek to limit or hinder the District of Columbia's ability to safeguard public safety. But there is ample evidence of the harm that surveillance technologies can do to our most vulnerable communities, and of the costs of failing to engage the public at the outset. Effective oversight of surveillance tools helps ensure that only vetted technologies are used, and only where the benefits outweigh the harms. It also reduces the risk of misuse and abuse, strengthens public trust in MPD and other District

³ See Laura Hautala, *These laws make police get public buy-in on surveillance tools*, CNET (May 28, 2019, 5:00 AM), <https://www.cnet.com/news/these-laws-make-police-get-public-buy-in-on-surveillance-tools/>; *Oakland Prioritizes Front-End Accountability on Privacy and Surveillance*, NYU SCHOOL OF LAW POLICING PROJECT (May 24, 2019), <https://www.policingproject.org/news-main/2019/5/17/oakland-prioritizes-front-end-accountability-on-privacy-and-surveillance>.

⁴ Section 3 of the bill.

⁵ Section 4 of the bill.

agencies, and increases participation from D.C. residents in policies that directly affect them.⁶

Front-end accountability of government surveillance will ensure transparent and optimized policies with public participation. Excluding the public from the decision-making process and failing to proactively disclose information regarding the use of surveillance tools will lead to drawn-out public records requests, lawsuits, and costly investigations.⁷ By including the public in surveillance oversight, D.C. can decrease costs, boost efficiency, and use public dollars most effectively.

In addition to front-end accountability, this bill provides for continued accountability through periodic auditing and reporting of surveillance technologies. D.C. agencies like the MPD have used a variety of surveillance technologies in the past and are increasing the testing and use of potentially wide-reaching technologies; ongoing reviews of the deployment and impact of those tools will be critical.

The MPD already uses a variety of surveillance tools; their effectiveness, public legitimacy, and responsible management would be bolstered by robust oversight and transparency legislation.

CCTV: D.C. currently has 5.6 cameras per thousand residents, making the list of the 50 most surveilled cities in the world.⁸ This past November, the City announced that it planned to nearly double the number of cameras on the streets, adding 140 cameras to the slate of 205 cameras already in use.⁹ Video cameras may operate in real time, or may record and save data for future review, and they can be outfitted with additional surveillance technologies, from license plate readers and gunshot detection to thermal imaging and biometric recognition.

⁶ See, e.g., President's Task Force on 21st Century Policing, *Final Report of the President's Task Force on 21st Century Policing*, DEP'T OF JUST. OFF. OF COMMUNITY ORIENTED POLICING SERVICES at 1, 35 (2015), https://www.eff.org/files/2018/10/02/taskforce_finalreport_1.pdf ("Law enforcement agencies should establish a culture of transparency and accountability in order to build public trust and legitimacy. This will help ensure decision making is understood and in accord with stated policy.").

⁷ See, e.g., Barry Friedman, *Democratic Policing Can Lead To More Accountability*, THE ALI ADVISER (Feb. 22, 2017), <http://www.thealiadviser.org/policing/democratic-policing-can-lead-accountability/>; see also Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance*, N.Y. TIMES (Oct. 13, 2013), <https://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html> (discussing how public outcry against an advanced surveillance technology program compelled the Oakland City Council to add restrictions to the use of surveillance technology, and noting that the "Seattle City Council forced its police department to return a federally financed drone to the manufacturer").

⁸ Emma Coleman, *Six U.S. Cities Make the List of Most Surveilled Places in the World*, CITY LAB (Sept. 19, 2019), <https://www.citylab.com/equity/2019/09/six-us-cities-make-list-most-surveilled-place-world/598426/>.

⁹ Lorenzo Hall, *Over 140 high-tech surveillance cameras are about to be installed in DC to help limit violence*, WUSA9 (Nov. 25, 2019), <https://www.wusa9.com/article/news/new-cameras-to-reduce-dc-violence/65-aa8901a0-7087-4186-b0d7-d05d069933d7>.

Notably, the evidence suggests that video cameras contribute to crime reduction in only a limited category of crimes;¹⁰ at the same time, surveillance cameras can be intrusive, chilling protected expression and assembly and hampering relations between law enforcement and the citizenry. And as with most types of surveillance technologies, they can be used to target enemies or to disproportionately surveil communities of color and other marginalized communities.¹¹ These risks point to the critical need for a robust oversight structure of the type that this legislation would provide.

Facial identification: There may be no more hotly contested surveillance tool at the moment than facial recognition technology. Several jurisdictions have enacted total bans on facial recognition, and a growing chorus is recognizing the risks of these systems.¹² In the meantime, reporting suggests that the District has withheld information about its use of facial recognition programs from Congress, further stymieing oversight.¹³

¹⁰ See, e.g., Eric L. Piza et al., *CCTV surveillance for crime prevention. A 40-year systematic review with meta-analysis*, 18 CRIMINOLOGY & PUB. POL'Y 135 (2019); U.S. GEN. ACCOUNTABILITY OFFICE, GAO-03-748, VIDEO SURVEILLANCE: INFORMATION ON LAW ENFORCEMENT'S USE OF CLOSED-CIRCUIT TELEVISION TO MONITOR SELECTED FEDERAL PROPERTY IN WASHINGTON, D.C. at 21 (2003) (“[D]emonstrating a direct cause and effect relationship between decreased crime and CCTV may not be easy to do.”); La Vigne et al., *Evaluating The Use Of Public Surveillance Cameras For Crime Control And Prevention*, URBAN INST. at 39–41, 79–82 (2011) (discussing that surveillance cameras contributed to crime prevention in some areas of Baltimore and Chicago, but did not reduce crime in Washington, D.C.); Brandon C. Welsh & David P. Farrington, *Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis*, 26 JUST. Q. 716, 736 (2009) (finding that surveillance cameras were most effective in reducing crime in car parks and vehicle crime and had little to no effect on other types of crime or crimes in broader public areas, and that some success was likely a result of other factors as well, such as improved lighting and security guards).

¹¹ *What's Wrong with Public Video Surveillance?*, ACLU, <https://www.aclu.org/other/whats-wrong-public-video-surveillance> (“For example, in 1997, a Washington DC police official was caught using police databases to gather information on patrons of a gay club.”); see also Avis Thomas-Lester & Toni Locy, *Chief's Friend Accused of Extortion*, WASH. POST (Nov. 26, 1997), <https://www.washingtonpost.com/wp-srv/local/longterm/library/dc/dcpolice/stories/stowe25.htm>.

¹² See Clare Garvie & Laura M. Moy, *America Under Watch-Face Surveillance in the United States*, GEO. L. CTR. ON PRIVACY & TECH. (May 16, 2019), <https://www.americaunderwatch.com/>; see also Angel Diaz, *Oversight of Face Recognition Is Needed to Avoid New Era of 'Digital Stop and Frisk'*, BRENNAN CTR. FOR JUSTICE (May 31, 2019), <https://www.brennancenter.org/our-work/analysis-opinion/oversight-face-recognition-needed-avoid-new-era-digital-stop-and-frisk>; Angel Diaz & Faiza Patel, *Face it: This is risky tech*, BRENNAN CTR. FOR JUSTICE (Aug. 16, 2018), <https://www.brennancenter.org/our-work/analysis-opinion/face-it-risky-tech>; Sigal Samuel, *San Francisco banned facial recognition tech. Here's why other cities should too*, VOX (May 16, 2019), <https://www.vox.com/future-perfect/2019/5/16/18625137/ai-facial-recognition-ban-san-francisco-surveillance>; Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), <https://www.perpetuallineup.org/>.

¹³ See *Facial Recognition Technology Regulation: A Practical Guide for Congress*, OPEN THE GOV'T at 3 (2019), <https://www.openthegovernment.org/wp-content/uploads/2019/07/Facial-Recognition-Technology-Regulation-A-Practical-Guide-for-Congress-1.pdf> (“In Washington, D.C., police withheld records from members of Congress on their use of facial recognition technology because their agreements with the company, MorphoTrak, were stamped ‘Confidential and Proprietary.’”).

As an initial matter, facial recognition technology can be enormously intrusive: an accurate, real-time identification tool would enable a police officer to instantly target an individual at a protest, identify everyone in a group, or even recognize people from afar while they walk down the street. While we take the risk that we may not remain entirely anonymous when we walk around in public, the use of these tools to effortlessly identify individuals poses unprecedented risks to the rights of speech and assembly and to the ability to remain functionally anonymous when desired.¹⁴ Indeed, recent revelations about the use of a facial recognition tool by law enforcement led to a swift backlash from the public and elected officials.¹⁵

At the same time, there are demonstrated flaws in the accuracy of these systems, particularly when it comes to identifying individuals of color, women, and the elderly. For example, in a test on members of Congress using Amazon's facial recognition tool Rekognition, the software incorrectly matched 28 members of Congress to a mug shot database, with people of color making up a disproportionate number of those falsely identified.¹⁶ In a similar vein, a study by the Algorithmic Justice League found that female subjects or individuals with darker skin tones made up the majority of faces that were misgendered or wrongly identified by Microsoft and Face++ (a company offering a gender classification product).¹⁷

Concerns about the inaccuracy, intrusiveness, and misuse of facial recognition tools make it especially critical that the public and the D.C. Council have insight into the use of these tools by the MPD.¹⁸ The Surveillance Impact Report outlined in the bill would provide vital information about any potential facial recognition tool and its impact on the communities of color and immigrant communities most likely to be affected and improperly identified by such a tool. This process would allow the D.C. Council to

¹⁴ See, e.g., *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (“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.”).

¹⁵ See Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>; Corinne Reichert, *Clearview AI sued over facial recognition privacy concerns*, CNET (Jan. 24, 2020 4:29 PM), <https://www.cnet.com/news/senator-demands-answers-from-clearview-ai/>.

¹⁶ Jacob Snow, *Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU (July 26, 2018), <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>

¹⁷ *Results*, GENDER SHADES, <http://gendershades.org/overview.html>.

¹⁸ Somerville, MA and San Francisco, CA have already instated city-wide bans on the technology. See Katya Schwenk, *Facial recognition technology is here to stay, say analysts*, STATE SCOOP (July 1, 2019), <https://statescoop.com/facial-recognition-technology-is-here-to-stay-say-analysts/>.

receive informed recommendations from the Privacy Advisory Committee regarding whether to approve and implement a facial recognition system.¹⁹

Stingrays: Cell site simulators, often referred to as Stingrays, force nearby cell phones to connect through them by mimicking cell phone towers, allowing the person operating the simulator to identify the phone numbers associated with nearby mobile devices or to locate individuals in the vicinity with pinpoint accuracy.²⁰ Multiple courts – including, in 2017, the D.C. Court of Appeals – have held that Stingrays are so privacy-invasive that law enforcement must obtain a warrant to use one.²¹ Providing more information about Stingrays and similar technologies at the outset would help ensure that the MPD puts appropriate measures in place to protect citizens’ constitutional and privacy rights before they are deployed in the field, avoiding costly litigation and decreasing the risk that important evidence will be suppressed as a result of defects underlying its collection.

Other surveillance technologies: The District also reportedly uses automated license plate readers to scan hundreds of millions of license plates per year, though police department representatives have notably declined to provide additional information about their deployment or oversight.²² These devices raise questions about police departments’ partnerships with private companies like Vigilant Solutions, as well as contracts with ICE to track the movements of undocumented individuals; enhanced reporting obligations would help elicit this information in advance to determine whether and how to implement those tools, and back-end audits would assist the public in ensuring that the costs of these tools – both financial and societal – are carefully managed and mitigated.²³

Similarly, body-worn cameras, implemented in 2015 to promote accountability, community relations, and safety, have not met these goals due to non-compliance with District policies as well as other failures in implementation. A robust review process at

¹⁹ Section 8 of the bill.

²⁰ See *Stingray Tracking Devices: Who’s Got Them?* ACLU (Nov. 2018), <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them>.

²¹ *Prince Jones v. United States*, No. 15-CF-322 (D.C. Sept. 21, 2017); see also *Carpenter v. United States*, 138 S.Ct. 2206 (2018) (holding police must get a warrant before obtaining seven or more days of cell site location information); *Tracey v. State*, 152 So. 3d 504 (Fla. 2014) (finding that people have a reasonable expectation of privacy in their cell site location information).

²² Martin Austerhuhle, *License to track? D.C. Cameras Capturing Millions Of License Plate Numbers*, WAMU.org (Dec. 10, 2013), https://wamu.org/story/13/12/10/license_to_track_dc_police_cameras_capturing_millions_of_license_plate_numbers/.

²³ See, e.g., Angel Diaz & Rachel Levinson-Waldman, *Hold private police partners accountable, too: For-profit companies are making millions with special access to NYPD information*, NY DAILY NEWS (Oct. 26, 2018 5:00AM), <https://www.nydailynews.com/opinion/ny-oped-hold-private-police-partners-accountable-too-20181025-story.html>; Vasudha Talla, *Documents Reveal ICE Using Driver Location Data From Local Police for Deportations*, ACLU (Mar. 13, 2019), <https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data>.

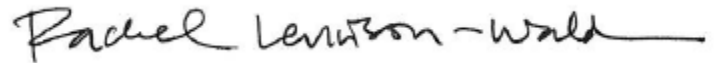
the outset, coupled with the establishment of regular reviews and audits, could have helped to mitigate some of these problems.²⁴

* * * * *

The goal of surveillance transparency and accountability efforts is to front-load oversight, allowing policymakers and community members to have an informed conversation about the rules of the road before the MPD or another D.C. agency deploys a new technology and before another alarming headline emerges about police surveillance. These efforts would also facilitate the provision of information that individuals or public interest organizations might otherwise have to devote months or even years to obtaining via public records requests and lawsuits.²⁵ Rather than a pattern of “suspicion and scandal,” front-end protections can augment safety and community involvement by putting in place critical safeguards on surveillance technologies, ensuring a regular flow of information, and encouraging the District to be thoughtful in how it approaches new surveillance technologies.²⁶ This approach can help prevent harms to individual rights, strengthen community trust, and avoid wasting scarce resources.

We urge the Council to schedule a public roundtable for further discussion regarding the state of surveillance in the District. Please do not hesitate to contact me if we can be of additional assistance; I can be reached at 202-249-7193 or levinsonr@brennan.law.nyu.edu.

Sincerely,



Rachel Levinson-Waldman
Senior Counsel, Liberty and National
Security Program

CC: At-Large Councilmember Anita Bonds
Councilmember Mary M. Cheh

²⁴ See Nassim Moshiree, *ACLU-DC Statement at Public Oversight Roundtable on “Five Years of the Metropolitan Police Department’s Body-Worn Camera Program: Reflections and Next Steps,”* ACLU (Oct. 21, 2019), <https://www.acludc.org/en/legislation/aclu-dc-statement-public-oversight-roundtable-five-years-metropolitan-police-departments>.

²⁵ See, e.g., *NYPD Predicting Policing Documents*, BRENNAN CTR. FOR JUSTICE (July 12, 2019), <https://www.brennancenter.org/our-work/research-reports/nypd-predictive-policing-documents>.

²⁶ See Michael Price, *Fact Check: The POST Act & National Security*, BRENNAN CTR. FOR JUSTICE (Mar. 6, 2017), <https://www.brennancenter.org/sites/default/files/170302%20-%2020-Pager%20on%20National%20Security%20Impact%20FINAL2.pdf>.

Councilmember Vincent M. Gray