

**Testimony on Behalf of New America's Open Technology Institute before the
D.C. Council Committee on the Judiciary and Public Safety**

Performance Oversight Hearing

By Lauren Sarkesian

Thursday, March 11, 2021

Chairman Allen and Members of the Committee:

My name is Lauren Sarkesian, and I am a Senior Policy Counsel at New America's Open Technology Institute (OTI). Thank you for the opportunity to testify today.

OTI works to ensure that every community has equitable access to technology and its benefits. This includes working to ensure that government surveillance is subject to robust safeguards that protect individual rights. OTI is based here in the District, and we address both federal and local laws and policies.

First, we would like to applaud the efforts that the Committee is undertaking to address police reform in the District. The police killings of George Floyd, Breonna Taylor, and others last year—which follow a long history of police brutality toward Black people—spurred an overdue reckoning over racial justice and the role of police in our country. We are glad that the Committee and the Council responded swiftly and continue with ongoing efforts toward police reform.

As a next step in these efforts, it is crucial that the Committee and the Council rein in police use of surveillance technologies. While it is important to directly address police conduct and accountability, legislative efforts should also account for the fact that technology tools are rapidly spreading, and contribute to the disproportionate policing in the United States. Increasingly over the past two decades, police departments across the country have been acquiring, deploying, and gaining access to surveillance equipment in secret, without any notice to the public or authorization from local legislatures-- including here in the District.

Studies have shown that technologies like facial recognition are biased against women and people of color,¹ and in fact, we now have numerous clear examples of cases in which facial recognition mismatches led to the wrongful arrests of Black men.² But even

¹ Buolamwini and Gebru. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification (2018), <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

² Kashmir Hill, *Wrongfully Accused by an Algorithm*, NY Times (Jun. 24, 2020), <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>; Kris Holt, *Facial recognition linked to a second wrongful arrest by Detroit police*, Engadget (July 10, 2020), <https://www.engadget.com/facialrecognition-false-match-wrongful-arrest-224053761.html>.

as these powerful technologies improve in terms of accuracy, they pose profound threats. Police surveillance technologies are extremely privacy invasive, as they provide the government an unprecedented ability to monitor local residents over time, and accumulate vast amounts of their personal data. Surveillance technologies are also prone to abuse and disproportionately used on communities of color,³ leading to higher arrest rates in those communities and feeding the cycle of racialized policing.⁴

First Amendment rights are also at stake. As Black Lives Matter protestors pushed for racial justice in the District and across the country last year, reports surfaced that they were subject to mass surveillance, via a wide array of these technologies.⁵ Biometric surveillance technologies can track thousands of protesters from each surveillance camera—and MPD has hundreds of CCTV cameras across the District.⁶

So, these threats are not hypothetical, nor are they remote. We know that the MPD uses facial recognition technology, cell-site simulators, and automated license plate readers, among other surveillance tools.⁷ But we lack complete information about MPD's technologies, and the policies that govern their use. And because of the very real threats they pose, surveillance technologies should not be funded, acquired, or used without at least community input and very clear, specific approval by the Council.

For these reasons, OTI is a member of the Community Oversight of Surveillance -- DC (COS-DC) coalition, a local coalition of groups working to secure legislation in the District that would provide transparency and accountability for D.C. government use of surveillance technologies.⁸ The legislation we seek would ensure that D.C. residents

³ See e.g., Brian Barret, *The Baltimore PD's Race Bias Extends to High-Tech Spying, Too*, Wired (Aug. 16, 2016), <https://www.wired.com/2016/08/baltimore-pds-race-bias-extends-high-tech-spying/>; Adam Goldman and Matt Apuzzo, *NYPD Defends Tactics over Mosque Spying; Records Reveal New Details on Muslim Surveillance*, Huffington Post (Feb. 25, 2012), http://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over_n_1298997.html;

Dave Mass & Jeremy Gillula, *What You Can Learn From Oakland's Raw ALPR Data*, EFF (Jan. 21, 2015), <https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data>.

⁴ See Rashida Richardson, Jason Schultz & and Kate Crawford, *DIRTY DATA, BAD PREDICTIONS: HOW CIVIL RIGHTS VIOLATIONS IMPACT POLICE DATA, PREDICTIVE POLICING SYSTEMS, AND JUSTICE* (Feb. 13, 2019), 94 N.Y.U. L. REV. ONLINE 192 (2019), available at SSRN: <https://ssrn.com/abstract=3333423> (discussion of predictive policing technology's threats to rights resulting from the software perpetuating existing and historic racialized policing).

⁵ Rebecca Heilweil, *Members of Congress Want to Know More About Law Enforcement's Surveillance of Protestors*, Vox (Jun. 10, 2020), <https://www.vox.com/recode/2020/5/29/21274828/drone-minneapolis-protests-predator-surveillance-police>.

⁶ Deirdre Paine, "DC to Spend \$5 Million for Additional 140 Security Cameras Around City." The DC Post, Nov. 27, 2019, <https://thedcpost.com/washington-dc-5-million-new-security-cameras/>.

⁷ See e.g., Letter from Chief of Police Cathy L. Lanier to Councilmember Charles Allen, (March 2, 2020), <https://dccouncil.us/wp-content/uploads/2020/03/JPS-Performance-Oversight-Responses-2020-MPD.pdf> (confirming the Metropolitan Police Department's use of facial recognition technology, automatic license plate readers and cell site simulators in response to Committee and questions); see also, Lauren Sarkesian and Maria Angel, *Debate on Police Surveillance Technologies in D.C. Is Long Overdue* (Sept. 10, 2020), <https://www.newamerica.org/oti/blog/debate-police-surveillance-technologies-dc-long-overdue/>.

⁸ Community Oversight of Surveillance DC, <https://takectrldc.org/> (last visited Oct. 16, 2020).

and the D.C. Council have a say in whether, when, and how particular technologies are used.

Nineteen jurisdictions across the country have enacted these “Community Control Over Police Surveillance” (CCOPS) bills over the past few years to provide much needed transparency and accountability for local government surveillance.⁹ The District should be next. As our nation’s capital, Washington, D.C. has long been a central place for protest in the United States. District residents need protection from inappropriate surveillance both as we exercise our First Amendment rights, and day-to-day.

Fundamentally, the legislation we urge the Council to pursue would require the D.C. government to:

- Use a transparent public process when any D.C. government agency seeks to acquire and use any surveillance technology and only allow use of technologies that have clear approval from the Council.
- Weigh costs and benefits to the District regarding technology the Council is considering, including impact on individual civil rights and civil liberties.
- Establish written use policies for each surveillance technology, which must be approved by the Council before use.
- Create a surveillance advisory committee that would advise government agencies and the Council on surveillance technologies.
- Conduct regular audits and evaluations of the use and impact of surveillance technologies, including the impact on rights and liberties.

This legislation would ensure that tough decisions surrounding police technologies are shared between the government and the community, and would set up clear processes to safeguard residents’ rights. These processes, and the transparency they would bring to our policing, could therefore ensure that we think carefully about how we invest in our community’s public safety, and could also help to build trust between the community and police—goals we know this Committee shares.

Accordingly, we ask that the Committee consider surveillance-related legislation as soon as possible as part of your comprehensive police reform efforts. Both OTI and our COS-DC coalition stand ready to help in these matters. Thank you.

⁹ COMMUNITY CONTROL OVER POLICE SURVEILLANCE, ACLU (last visited Oct. 16, 2020), <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance>; Mailyn Fidler, *Fourteen Places Have Passed Local Surveillance Laws. Here’s How They’re Doing*, Lawfare Blog, Sept. 3, 2020, <https://www.lawfareblog.com/fourteen-places-have-passed-local-surveillance-laws-heres-how-theyre-doing>.