Statement on behalf of
New America's Open Technology Institute
before the
D.C. Council Committee on the Judiciary and Public Safety
Performance Oversight Hearing on the Metropolitan Police Department
January 16, 2020
by
Sharon Bradford Franklin, Policy Director

My name is Sharon Bradford Franklin, and I am the Policy Director of New America's Open Technology Institute (OTI). Thank you for the opportunity to testify at today's hearing.

OTI works to ensure that every community has equitable access to digital technology and its benefits. This includes working to ensure that government surveillance is subject to robust safeguards that protect individual rights and provide accountability. In particular, OTI promotes measures that will provide transparency and an opportunity for public input regarding the rules governing the operation of surveillance programs. OTI is based here in Washington, D.C., and we address both federal and local laws and policies.

Increasingly over the past two decades, police departments and other government agencies in localities across the country have been buying and installing surveillance equipment without any notice to the public or even approval from local legislatures.[1] These technologies range from more traditional CCTV cameras to facial recognition systems to police body cameras and license plate readers. These powerful surveillance technologies can give government the ability to monitor local residents over time, and accumulate vast amounts of personal data. While there are valid law enforcement purposes for relying on particular technological tools in certain circumstances, it is critical that local residents and their elected representatives have a say in whether and how any surveillance system is used in their jurisdiction. Studies have shown that technologies like facial recognition are biased against women and people of color,[2] and pervasive use of any surveillance technology can chill free speech and create

[1] Robyn Greene. "How Cities are Reining in Out-of-Control Policing Tech." *Slate: Future Tense*, May 14, 2018, https://slate.com/technology/2018/05/oakland-california-and-other-cities-are-reining-in-out-of-control-police-technologies.html

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

oppressive environments. Accordingly, surveillance technologies should not be funded, acquired, or used without community input and very clear, specific approval by the local legislature.

The good news is that in the past few years, local communities across the country have begun to enact legislation to provide much needed transparency and accountability for local government surveillance programs. In September of 2016, the ACLU and partners, including my organization, the Open Technology Institute, launched the Community Control Over Police Surveillance (CCOPS) effort.[3] The purpose of CCOPS is to ensure that residents and lawmakers are empowered to decide whether and how surveillance technology is acquired and used by local law enforcement agencies. To date, thirteen cities and counties in California, Massachusetts, Ohio, Tennessee, and Washington state have adopted local laws based on the CCOPS model, and dozens of other jurisdictions are considering similar proposals.

OTI is a member of the Community Oversight of Surveillance -- DC (COS-DC) a local coalition of groups based in Washington, D.C., that is working to secure enactment of legislation here in the District to provide this type of transparency and accountability for government use of surveillance technologies. As I will briefly explain in a moment, the COS-DC legislation would not ban any particular type of technology, but would instead ensure that D.C. residents and the D.C. Council have a say in whether, when and how particular technologies are used.

Here in the District, the Metropolitan Police Department (MPD) has long operated a network of CCTV cameras, with some degree of oversight by the D.C. Council and transparency to the public. However, there has not been sufficient oversight or transparency for the MPD's CCTV system, and other D.C. government surveillance programs have been subject to even less accountability. For example, just this past November, the Mayor announced that MPD would be adding 140 additional CCTV cameras,[4] without providing any prior notice to the D.C. Council, even though the Council had considered and adopted new rules for the CCTV program just one month earlier. And without any clear rules in place to require public accountability, there is almost no publicly available information with regard to the District's use of many other surveillance technologies.

---

[3] ACLU. Community Control Over Police Surveillance, accessed on Jan. 14, 2020, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance

[4] Deirde 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/

The MPD's acquisition of Stingrays illustrates clearly why it is critical that the District enact the Community Oversight of Surveillance-DC legislation. Stingrays, otherwise known as cell site simulators, are devices that simulate the operation of cell towers and capture information from nearby cell phones. Police using these devices can pinpoint the location of cell phones, and some Stingray devices also enable police to intercept calls and listen to their content. Investigative reporting shows that MPD acquired Stingrays through a federal grant in 2003, and sought to use the devices starting in 2008.[5] But there is almost no public information available regarding how MPD has actually used Stingrays. Nor is there any public record showing any consideration or oversight of MPD's Stingray use by the D.C. Council.

Similarly, there are not sufficient rules in place to ensure accountability for MPD's efforts to expand the coverage of its CCTV cameras through networks with private security cameras. According to MPD's latest data (dated December 31, 2019) 17,408 private security cameras have been funded under MPD's Private Security Camera Incentive Program since the program's inception in 2016.[6] The program, which incentivizes residents to install private security cameras and register them with MPD (for a maximum $500 rebate per residential address, or for free if qualifying under the Voucher Program) adds a new fleet of surveillance cameras all over the city, thereby allowing MPD to greatly expand its CCTV reach, with little oversight. While there can be security benefits to installing cameras on homes, businesses, and places of worship, MPD must remain accountable to the public even when it relies on footage from private cameras. We must ensure that there is a process in place that determines when and how MPD has access to this video surveillance footage, and that the community has had sufficient input into that process.

The D.C. Council should enact legislation to provide transparency, oversight and accountability for the use of surveillance technologies by any District government entity. Our coalition has developed a proposed bill that is D.C. specific but relies on models provided by the thirteen jurisdictions that have already enacted this type of legislation. Although the legislation adopted in these communities has varied to some degree, there are some common elements that are also key components of our COS-DC bill.

---

[5] Jason Leopold. "Police in Washington, DC Are Using the Secretive 'Stingray' Cell Phone Tracking Tool." *Vice News*, Oct. 17, 2014, https://www.vice.com/en_us/article/yw4jqv/police-in-washington-dc-are-using-the-secretive-stingray-cell-phone-tracking-tool

[6] DC Office of Victim Services and Justice Grants. January 2020 Private Security Camera System Incentive Program Report, accessed on Jan. 14, 2020, https://ovsjg.dc.gov/sites/default/files/dc/sites/ovsjg/service_content/attachments/January%202020.pdf

These key components, include:

1. Transparent public process: Whenever MPD or any other D.C. government agency seeks to acquire and use any surveillance technology, they would be required to obtain Council approval following a public hearing.

2. Council must weigh costs and benefits to the District, including safeguards for individual rights, in determining approvals: Under this legislation, the D.C. Council would determine whether to approve any particular surveillance technology based on weighing the costs and benefits to the community, and assessing whether there are adequate safeguards for civil rights and civil liberties.

3. Written rules for use of surveillance technologies: D.C. government agencies would be required to develop written rules that govern when and how they may use surveillance technologies and submit the rules to the D.C. Council for approval. These include surveillance impact reports that explain how a technology works and will impact the community, and surveillance use policies that set out specific guidelines for the technology's use by the agency.

4. Privacy Advisory Group: The bill would require creating a privacy advisory group to advise and help inform both D.C. agencies and the Council on civil rights and civil liberties risks of specific surveillance technologies and their use in the District. This group would include representatives from local D.C. communities, and people with expertise in privacy and technology.

5. Regular audits and evaluations: The bill would require regular periodic assessments and annual evaluation of the District's use of surveillance technology to ensure that costs–both to residents and to their rights–do not outweigh any potential benefits, and to assess whether D.C.'s use of surveillance technology furthers public safety goals.

Conclusion:

The District should be the next jurisdiction to enact much-needed legislation to provide transparency and accountability for government use of surveillance technologies. As I noted earlier, the legislation would not ban surveillance technologies, but would instead ensure that decisions about their use are made with thoughtful consideration and buy-in from the public and elected lawmakers, and that the operation of approved technologies will be subject to rules that safeguard residents' rights and provide transparency.

To begin the process of considering the COS-DC legislation, we join with coalition members in asking 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, both intended and unintended, of unchecked government surveillance and inform a path forward to solutions. The Open Technology Institute and our partners in the COS-DC coalition look forward to working with members of the Council in this effort.