BRENNAN
CENTER
FOR JUSTICE
TWENTY
YEARS

Brennan Center for Justice
at New York University School of Law

120 Broadway
Suite 1750
New York, New York 10271
646.292.8310 Fax 212.463.7308
www.brennancenter.org

June 14, 2017

Written Testimony of Michael Price, Counsel
Brennan Center for Justice at New York University Law School
Before the
New York City Council Committee on Public Safety
In Support of Int. 1482

Good afternoon, Chairwoman Gibson and members of the Public Safety Committee. My name is Michael Price and I serve as Counsel for the Brennan Center for Justice at NYU School of Law in the Liberty and National Security Program. Thank you for holding this hearing and inviting the Brennan Center to testify in support of Int. 1482, the Public Oversight of Surveillance Technology Act. And thank you once again to Councilmembers Daniel Garodnick and Vanessa L. Gibson for co-sponsoring this important reform.

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 focuses on helping to safeguard our constitutional ideals in the fight against terrorism. As a part of that work, we advocated for the creation of an Inspector General for the NYPD in 2013, following the NYPD's well-documented and unconstitutional surveillance of Muslim communities. And we continue to seek greater transparency and oversight of NYPD surveillance practices, including the use of powerful new technologies that present profound concerns for civil rights and civil liberties, now more than ever. That is why the Brennan Center is proud to support the POST Act here today.

The Brennan Center commends the Council on its thoughtful approach to balancing the need for democratic oversight and transparency with the NYPD's legitimate need for operational secrecy. Although the NYPD may not wish to discuss the surveillance tools they use, a strong local democracy like New York City requires at least a basic level of information about what its local police are doing and how they're doing it. The POST Act will inform the public – and critically, members of the City Council – about the kinds of information the NYPD collects and the policies in place for retaining, sharing, and protecting it. It also carefully avoids the disclosure of operational details that might compromise police investigations or harm public safety.

Specifically, the bill would require the NYPD to create an "impact and use policy" for surveillance technologies now in use as well as any new technologies that come along in

the future. The requirement would cover devices like "Stingrays" (cell phone locators),[1] automatic license plate readers,[2] and mobile "X-ray" vans.[3] It would also include software like automated facial recognition programs[4] as well as information sharing networks like the $40 million Domain Awareness System, which combines information from NYPD records and databases with the thousands of public and private security cameras that blanket the city.[5] Reports would have to describe what the technology does as well as the policies and procedures for using it, like whether a warrant or court order is necessary. They would also describe the rules for using or sharing[6] the information collected as well as safeguards to prevent unauthorized access, whether training is required, and any internal compliance procedures.

Such information is essential to effective public oversight, but it is too general to be a tool for those who might wish to evade lawful police surveillance. It does not provide any information about how the NYPD uses the technology in connection with specific investigations or types of investigations. It does not disclose where or when it might be used or how someone might defeat it. It also does not make the tools any less effective. Wiretaps, for example, remain a potent investigative tool despite widespread knowledge of their existence and the strict rules for their use. Likewise, Stingrays will continue to work; X-ray vans will continue to see through cars and buildings, and license plate readers will continue to read license plates. Unless criminals and terrorists stop using cell phones and cars, these devices will be just as effective as they are today.

It is true that the NYPD might enjoy a brief advantage if it were to secretly acquire a new technology that is completely unknown to the public. But history shows that the public inevitably finds out, through costly Freedom of Information Law (FOIL) litigation, through the press, or through the courts. Indeed, law enforcement has an obligation to properly disclose information about its use of surveillance technologies to judges and

---

[1] Reuven Blau, "Here's how the NYPD's Stingray tech can spy on New Yorker's cell phones," *New York Daily News*, March 9, 2017, http://www.nydailynews.com/new-york/nypd-stingray-tech-spy-new-yorker-cell-phones-article-1.2992708.

[2] Mariko Hirose, "Documents Uncover NYPD's Vast License Plate Reader Database," *American Civil Liberties Union* (blog), January 25, 2016, https://www.aclu.org/blog/free-future/documents-uncover-nypds-vast-license-plate-reader-database.

[3] Conor Friedersdorf, "The NYPD Is Using Mobile X-Ray Vans to Spy on Unknown Targets," *Atlantic*, October 19, 2015, https://www.theatlantic.com/politics/archive/2015/10/the-nypd-is-using-mobile-x-rays-to-spy-on-unknown-targets/411181/.

[4] Claire Garvie and Alvaro Bedoya, "Smile! You've just been identified by face recognition," *New York Daily News*, March 27, 2017, http://www.nydailynews.com/opinion/smile-identified-face-recognition-article-1.3008512.

[5] Joe Coscarelli, "The NYPD's Domain Awareness System Is Watching You," *New York Magazine*, August 12, 2012, http://nymag.com/daily/intelligencer/2012/08/nypd-domain-awareness-system-microsoft-is-watching-you.html.

[6] The POST Act specifically requires the NYPD to disclose whether it shares data with outside agencies at the state and federal level. This is a critical feature of the bill that would assist New Yorkers in understanding how the NYPD shares information. Unfortunately, it does not require sufficient particularity regarding *which* federal agencies receive data. New Yorkers should know, for example, what data is being shared with ICE, directly or indirectly. The Brennan Center therefore recommends a more granular approach to Section 1(a)(6) that would require the NYPD to indicate which federal and state agencies are receiving or have access to NYPD data.

criminal defendants. The failure to do so can jeopardize thousands of investigations, as was the case in Maryland and Florida when investigators concealed their use of Stingrays from the courts by referring to them as a "confidential source."[7] Thus, even without this law, it is wishful thinking to suppose that the NYPD's surveillance tools would remain a secret for very long. The real question is when, not whether, the NYPD will need to acknowledge its use of new technologies.

The goal of the POST Act is to front-load that discussion, to have an informed conversation with policymakers and community stakeholders about the rules of the road *before* the NYPD deploys a new technology and *before* there is another alarming headline about police surveillance. Such a proactive approach provides an opportunity for up-front, constructive community input. It also encourages the NYPD to be thoughtful in how it approaches new surveillance technologies, so as not to engage in activities that harm individual rights, undermine its relationships with communities, or waste scarce resources.

This is a common sense idea embraced by law enforcement leaders. In 2015, President Obama's Task Force on 21st Century Policing specifically recommended that state and local law enforcement agencies "encourage public engagement and collaboration … when developing a policy for the use of a new technology."[8] According to the final report: "Local residents will be more accepting of and respond more positively to technology when they have been informed of new developments and their input has been encouraged. How police use technology and how they share that information with the public is critical."[9] Task Force co-chair Charles Ramsey also recognized that, "Just having the conversation can increase trust and legitimacy and help departments make better decisions."[10]

In fact, the federal government routinely discloses its ground rules for using new technologies. For example, both the Department of Justice[11] and the Department of Homeland Security[12] (DHS) have published policies on their use of Stingrays, requiring

---

[7] Nicky Wolf, "2,000 cases may be overturned because police used secret Stingray surveillance," *Guardian*, September 4, 2015, https://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance; Kim Zetter, "Emails Show Feds Asking Florida Cops to Deceive Judges," *Wired*, June 19, 2014, https://www.wired.com/2014/06/feds-told-cops-to-deceive-courts-about-stingray/.
[8] President's Task Force on 21st Century Policing, *Final Report od the President's Task Force on 21st Century Policing* (Washington, DC: Office of Community Oriented Policing Services, 2015), 35, https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf.
[9] Ibid.
[10] Ibid; *see also Privacy impact assessment report for the utilization of license plate readers* (Alexandria, VA: International Association of Chiefs of Police, 2009), 28, http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf. (recognizing that "[o]ne way to promote public confidence is to increase the transparency surrounding how [license plate reader] data will be managed by the law enforcement agency.").
[11] U.S. Department of Justice, *Department of Justice Policy Guidance: Use of Cell-site Simulator Technology*, https://www.justice.gov/opa/file/767321/download (accessed June 13, 2017).
[12] Alejandro N. Mayorkas, Memorandum to Sarah Saldana, et al., "Department Policy Regarding the Use of Cell-Site Simulator Technology," October 19, 2015, https://www.dhs.gov/sites/default/files/publications/Department Policy Regarding the Use of Cell-Site Simulator Technology.pdf.

agents to obtain a judicial warrant and apply important back-end privacy protections. DHS has also publicly described its use of backscatter x-ray systems for border security; issued Privacy Impact Assessments for use of facial recognition technology[13] and license plate reader data;[14] and issued guidance for state and local agencies using drones, which strongly recommended transparency and public outreach.[15] If the two federal agencies responsible for protecting our domestic national security can provide this type of information to the general public, then the NYPD can surely do so as well.

The NYPD may also discover that there are benefits to community engagement, as in Oakland, California, where police officials say they have helped build community trust through transparency and dialogue on surveillance technology issues.[16] Oakland police have already begun to implement an ordinance, widely expected to become law, which contains transparency reporting requirements comparable to the POST Act.[17] In preparation, police officials have begun attending public oversight meetings to provide information about the different surveillance technologies that Oakland uses, including Stingrays, and the privacy concerns they raise.[18] From a police perspective, sharing this information has helped build community relationships and trust where there was little before. Tim Birch, a former Oakland police officer and current head of the Oakland Police Department's Research and Planning team, now considers it "bizarre" that there is "a world in which we don't want the public to know what we are doing or what we are doing with it. What equipment we have or how we are using it."[19] In New York, by contrast, the NYPD has been secretly using Stingrays for years, and yet the Department continues to fight FOIL requests for information about how it uses the devices.[20]

---

[13] U.S. Department of Homeland Security, U.S. Customs and Border Protection, *Privacy Impact Assessment for the Facial Recognition Air Entry Pilot*, DHS/CBP/PIA-025 (March 11, 2015), https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp-1-to-1-facial-recognition-air-entry-pilot-march-11-2015.pdf (accessed June 13, 2017).

[14] U.S. Department of Homeland Security, U.S. Immigrations and Customs Enforcement, *Privacy Impact Assessment for the Acquisition and Use of License Plate Reader Data from a Commercial Service*, DHS/ICE/PIA-039 (March 19, 2015) https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-lpr-march2015.pdf (accessed June 13, 2017) .

[15] U.S. Department of Homeland Security, Privacy, Civil Rights & Civil Liberties Unmanned Systems Working Group, *Best Practices for Protecting Privacy, Civil Rights & Civil Liberties Liberties in Unmanned Systems Programs* (December 18, 2015), https://www.dhs.gov/sites/default/files/publications/UAS%20Best%20Practices.pdf (accessed June 13, 2017).

[16] Michael Price, "What Oakland police can teach the NYPD," *amNewYork* (blog), May 12, 2017, http://www.amny.com/opinion/what-oakland-police-can-teach-the-nypd-1.13624678.

[17] Oakland, Cal., The Surveillnace and Community Safety Ordinance (Jan. 5, 2016), *available at* https://www.documentcloud.org/documents/3253520-oak061975.html (Draft).

[18] "Privacy Advisory Commission – LIVE," City of Oakland video, from a city council meeting televised on August 11, 2016, http://oakland.granicus.com/MediaPlayer.php?publish_id=0891cb33-63f2-11e6-8170-f04da2064c47

[19] Cyrus Farivar, "Ex-Cop: it's 'bizarre' if we can't explain to public what our snooping gear does," *Ars Technica*, January 29, 2017, https://arstechnica.com/tech-policy/2017/01/how-an-ex-cop-tries-to-get-a-police-department-to-think-about-privacy/.

[20] Barbara Ross, "NYCLU sues the NYPD to get Stingray spyware info," *New York Daily News*, May 19, 2016, http://www.nydailynews.com/new-york/nyclu-sues-nypd-stingray-spyware-info-article-1.2643103.

New Yorkers all want the NYPD to keep New York City safe, but new surveillance technologies do not just capture information about the "bad guys." They affect the privacy rights of all New Yorkers, especially – and disproportionately – communities of color. Without some basic information about what these technologies do and how the NYPD is using them, lawmakers and government watchdogs, including the NYPD Inspector General, cannot oversee the NYPD or do their jobs effectively.

Transparency and oversight are essential features of a strong democracy, and the Brennan Center commends the Council and this Committee for addressing this critical and timely issue. The Brennan Center strongly supports Int. 1482 and we encourage the Council pass it quickly.

Thank you again for the opportunity to testify today. I am happy to answer any questions.