The Public Oversight of Police Technology (POST) Act & National Security

The Public Oversight of Surveillance Technology (POST) Act would provide New York City lawmakers and the public with a meaningful opportunity to understand and oversee decisions about the NYPD's acquisition and use of new surveillance technologies. Council members Daniel Garodnick and Vanessa L. Gibson carefully crafted this bill to balance law enforcement and national security concerns with the need for transparency and democratic accountability, and the Brennan Center is proud to support it. It is wishful thinking to suppose that the NYPD's surveillance tools will remain secret forever. The real question is when, not whether, the NYPD will need to acknowledge its use of new technologies and have a substantive conversation with the public about their use. The goal of the POST Act is to have a productive conversation on the front end, rather than reacting to the next sensational headline.

The POST Act Will Not Tip Off the "Bad Guys"

- Many of the surveillance technologies used by the NYPD are well known to the public already, including the use of "Stingray" cell phone locators and backscatter "X-ray vans." The POST Act requires the NYPD to disclose its *policies and procedures* for using such powerful surveillance tools – not operational details.
- None of the information required by the POST Act is granular enough to be of value to a potential terrorist or criminal. It does not require the NYPD to disclose information about where or when it uses surveillance tools. It does not require the NYPD to disclose how it might use them it in connection with specific investigations or types of investigations. It does not require the NYPD to disclose how someone might evade or defeat them. It will not make surveillance 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. Unless criminals and terrorists cease to use cell phones and modern transportation, Stingrays will continue to be effective; X-Ray vans will continue to peer through cars and walls; and license plate readers will continue to read license plates.

Federal Agencies Routinely Disclose Information about New Surveillance Technologies

- Federal agencies have been strongly encouraged to disclose information about their use of new surveillance technologies. Both the Department of Justice and the Department of

Homeland Security (DHS) have published policies on their use of Stingrays, requiring agents to obtain a judicial warrant and apply important back-end privacy protections.

- DHS has also publicly described its use of use of facial recognition technology, license plate reader data, and backscatter X-ray systems for border security. Additionally, it has issued guidance for state and local agencies using drones, which strongly recommended transparency and public outreach. If the two federal agencies responsible for protecting our national security can provide this type of information to the general public, then the NYPD can surely do so as well.
- The President's Task Force on 21st Century Policing has recommended that law enforcement agencies "encourage public engagement and collaboration, including the use of community advisory bodies, when developing a policy for the use of a new technology." And the International Association of Chiefs of Police has endorsed this approach as well. In fact, the NYPD itself undertook to obtain feedback from the public in rolling out body cameras for its officers.

Failure to Disclose Information Can Harm Law Enforcement

- The use of new surveillance technologies for investigations must be properly disclosed to courts and criminal defendants. The alternative would jeopardize thousands of investigations and prosecutions, as was the case in Maryland and Florida.
- In practice, New Yorkers almost inevitably find out about the NYPD's surveillance activities - but only after the technology is in place and in use. This pattern generates suspicion and scandal as opposed an orderly democratic process that allows communities to understand how technology is being used and critical safeguards.

New Yorkers all want the NYPD to keep New York City safe, so it is important to emphasize that the POST Act would not disclose information that could be used to thwart lawful police surveillance. At the same time, new surveillance technologies do not just capture information about the "bad guys." They affect the privacy rights of all New Yorkers, especially – and disproportionately – immigrants and 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. New Yorkers should not be left in the dark.