

Fact Check: The POST Act & National Security

The <u>Public Oversight of Surveillance Technology (POST) Act</u> would provide New York City lawmakers with a meaningful opportunity to understand and oversee decisions about the NYPD's acquisition and use of new surveillance technologies. It also provides an opportunity for public engagement in this process. It is a carefully crafted bill that balances law enforcement and national security concerns with the need for transparency and democratic accountability.

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

- The NYPD's use of some surveillance technologies is known to the public already, including "Stingray" cell phone locators and backscatter X-ray vans, but the privacy and civil liberties safeguards if any are not. 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 disclosed through the POST Act is granular enough to be of value to a potential terrorist or criminal. It is, however, necessary to facilitate informed policy discussions and local democratic oversight.
- Surveillance technology does not need to be completely secret to be effective. Unless
 criminals revert to carrier pigeons, Stingrays will continue to work. 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. The President's Task Force on 21st Century Policing 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." Even the International Association of Chiefs of Police has recognized 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."
- In this vein, the Department of Justice, including the Federal Bureau of Investigation and Drug Enforcement Agency, has published policies on its use of Stingrays and surveillance drones.
- Likewise, the Department of Homeland Security has published a policy on its use of Stingrays. It has also publicly described its use of backscatter x-ray systems for border security; issued Privacy Impact Assessments for use of facial recognition technology and license plate reader data; and issued guidance for state and local agencies using drones, which strongly recommended transparency and public outreach.

Failure to Disclose Information Can Harm Law Enforcement

- In practice, New Yorkers <u>inevitably find out</u> 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.
- 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 <u>Baltimore</u> and <u>Florida</u>, where the police attempted to deceive courts and defense attorneys. Conversely, public awareness of the NYPD's capabilities may deter would-be terrorists and criminals in the same way as officer presence in certain locations.
- Affirmative disclosure of basic information about new surveillance technologies could save
 the City from costly Freedom of Information Law (FOIL) lawsuits or Federal
 Communications Commission (FCC) litigation, as in <u>Maryland</u>.

National security concerns must be treated with utmost seriousness. The POST Act promotes public safety and strengthens democratic values, allowing police to use the potent tools at their disposal while providing New Yorkers with an opportunity to weigh in on what is being done in their name.