Written by **Bob Adelmann** on February 12, 2016

NYPD "Stingray" Use Exposed by the NY Civil Liberties Union

In November the New York Civil Liberties Union (NYCLU) received part of what it requested from the New York Police Department under the Freedom of Information Act: What is "stingray," and how often are you using it, and under what conditions and restraints?

The rest of the information requested arrived earlier this week, and NYCLU went public with what it found.

A "stringray" is a cellphone tracking device that was originally developed for the military and intelligence community that fools cellphones into thinking the device a cell tower, inviting them to link to it. Through triangulation, stingrays can pinpoint the exact location of the cell phone.

The device can pick up other cellphones in the immediate area, along with outgoing calls and texts from the targeted cellphone.

What upset the NYCLU the most is that the NYPD has been using the device for years, in secret, and using it without getting the necessary search warrants as required under the Fourth Amendment:

> The NYPD disclosed [that] it used Stingrays nearly 1,106 times between 2008 and May of 2015 without a written policy and following a practice of obtaining only lower-level court orders rather than [search] warrants.
>
> This is the first time the extent of the use of Stingrays by the NYPD has been made public.

The NYCLU described how the NYPD was able to skirt Fourth Amendment protections:

> The NYPD['s] … practice is to obtain a "pen register order" — a court order that is not as protective of privacy as a [Fourth Amendment search] warrant — prior to using the device.
>
> The legal standard [under the Fourth Amendment] … is probable cause, but in order to obtain a pen register, the NYPD needs only to establish that the information [being sought] is "relevant to an ongoing criminal investigation."

Spokesmen for the NYPD immediately charged that the disclosure by the NYCLU was "misleading" in that in actuality it used a higher standard than "relevancy" or "reasonable suspicion" and that it restricted itself just to capturing the location of the targeted cellphone and nothing more. Chief Kerry Sweet, the commanding officer of the NYPD's legal bureau, explained: "We get the number and that's it. We do not pick up information from other people standing [near]by, innocent bystanders, passersby. [The Stingray] does not lock on their phone and pick [up] any information from their phones."

Another NYPD spokesman, Jonathan David, offered an explanation as to why the use of Stringrays had been kept secret for so long:

> The public disclosure of such information would allow terrorist actors and other potential investigative subjects to develop and implement countermeasures to these … tools.

Still another NYPD spokesman, J. Peter Donald, told ArsTechnica, a technology website:

> The NYPD, before using [a Stingray], ensures that we have established probable cause, consults with a District Attorney, and applies for a court order, which must be approved by a judge.…
>
> The NYCLU maligned that the privacy of New Yorkers is at risk. It is not. What is at risk is the safety of New Yorkers, without the limited use of this technology to locate dangerous fugitives.

This is counter to what Cyrus Farivar at ArsTechnica discovered: While most of those 1,016 Stingray uses involved investigations of serious felonies such as homicide, assault, kidnapping, drug trafficking, and rape, they were also used for investigating money laundering and ID theft. It was also counter to what the NYCLU uncovered during its look into the matter. The Erie County Sheriff's Office, located in western New York State, had used Stingrays 47 times in the last four years and only once had obtained a pen register order before doing so.

The issue is headed to an appeals court, which hopefully will settle the matter and stuff the Stringray genie back into the bottle. In 2013, two Milwaukee police officers, apparently using a Stingray, found their target, Damian Patrick, sitting in the front seat of a friend's car. They conducted a traffic stop — the car was already parked behind a house in suburban Milwaukee — and ordered Patrick and his friend out of the car. The officers then searched the car, again apparently without a warrant or permission, and found a semi-automatic handgun on the floor of the vehicle. As Patrick had an outstanding arrest warrant, they arrested him and took him into custody.

The arrest reports were vague, referring to an "unknown source" and "prior knowledge" that told them where Patrick was. Patrick filed suit claiming that the police couldn't have known where he was or had reasonable suspicion to arrest him.

The case, *United States v. Patrick*, has reached the 7th Circuit Court of Appeals, with Patrick's attorneys claiming,

> Cell-site simulators [like Stingray] raise especially serious questions under the Fourth Amendment, and at least require a warrant. Use of a cell-site simulator constitutes a search for several reasons.
>
> First, the device can precisely locate and track people's phones, which requires a warrant for the same reasons that tracking by the service provider does.
>
> Second, cell-site simulators transmit probing electronic signals through the walls of homes, offices, and other private spaces occupied by the target and innocent third parties in the area, and thereby force phones to transmit data to the government that reveals where inside those spaces the phones are.

Donna Lieberman, executive director of the NYCLU, noted the risks of only slightly limited surveillance to New Yorkers:

> If carrying a cell phone means being exposed to military grade surveillance equipment, then the privacy of nearly all New Yorkers is at risk.
>
> Considering the NYPD's troubling history of surveilling innocent people, it must at the very least establish strict privacy policies and obtain [Fourth Amendment search] warrants prior to using intrusive equipment like Stingrays that can track people's cell phones.

The Fourth Amendment must continue to be vigorously defended. Otherwise "mission creep" will eventually allow every agency in the country to surveil everyone, everywhere, all the time.

A graduate of an Ivy League school and a former investment advisor, Bob is a regular contributor to The New American *magazine and blogs frequently at LightFromTheRight.com, primarily on economics and politics. He can be reached at badelmann@thenewamerican.com.*

Related article:

Could the Third Amendment Thwart the Surveillance State?