Stingray Technology Shows Ongoing Tension Between Privacy Rights And Safety

Joshua Withrow

February 23, 2017

Law enforcement is always looking for the best new technology to stay one step ahead of increasingly sophisticated criminal agents, not to mention terrorist sympathizers.

In the pursuit of this goal, new surveillance equipment makes tracking actual criminal suspects easier and faster each year. Each advance in the field of surveillance stretches the boundaries of Fourth Amendment protections against undue search and seizure, creating grey areas where the legitimate pursuit of public safety may conflict with individuals' immediate privacy and right to be presumed innocent. In these cases, there should be a robust public debate to decide where to set that line.

Enter the Stingray. Properly known as an international mobile subscriber identity (IMSI) catcher, Stingray is the brand name of such a device that basically collects communications data over a wide area by tricking mobile devices into thinking that the Stingray is actually a cellphone tower. Stingrays can thus be used to track all nearby phones — and the creatures that carry them — in real time. Not only can this track your location, but it can also collect your metadata, such as what numbers are calling into the device. Furthermore, some Stingray devices appear to be able to collect actual *content* – i.e., your phone conversations, text messages, and the like.

Clearly this is powerful technology and was originally developed for military use overseas. However, the FBI began acquiring the devices for its agents as well as helping local and state law enforcement units acquire them, too.

It is not hard to imagine the legitimate usefulness of such a device in the case of an actual real-time crime investigation or a stakeout. However, the ability of these devices to track and intercept data from these devices *en masse* also raises due process concerns, especially if they are used for passive, ongoing surveillance. rather than targeted use at the behest of a court order.

Yep, the tax man can track you and listen to your phone calls.

Rather than have a debate over how these devices should be employed in public, a congressional inquiry released late in 2016 reveals that the FBI arranged for law enforcement to acquire these Stingray devices in secret. The FBI even conditioned the transfer of these devices on signing

non-disclosure agreements — to the point of demanding that the departments using these devices refuse to acknowledge their existence in court!

As the Cato Institute's Adam Bates documents in a major new study, many of the agencies that bought Stingrays did not have any formal guidelines for how to use them legally in the field until a series of leaks began tipping civil liberties activists to their existence. More disturbingly, there have been documented instances where law enforcement was forced to drop cases against a suspect to avoid revealing the evidence collected via Stingrays, and the FBI has even been caught directing police to invent alternate ways that Stingray data might have been collected constitutionally (a practice known as "parallel construction").

Just as concerning is the acquisition and use of Stingrays by executive branch agencies outside of the FBI. The most ridiculous example pointed out by the Oversight report is the IRS, which owns two Stingray devices and admitted to using them in 37 investigations so far. Yep, the tax man can track you and listen to your phone calls. Interestingly, the IRS devices have thus far been used mostly in cases involving non-tax crimes, leading one to wonder why such investigations aren't just being handed off to the FBI or other actual law enforcement bodies.

The combination of the massive potential for these devices to be used unconstitutionally to conduct mass surveillance, combined with the eyebrow-raising secrecy with which they have been acquired and used, merits congressional action.

It seems redundant to have to pass a federal law to specify that law enforcement needs to have a valid warrant to collect and use surveillance data against Americans in the U.S., but such is the state of the Fourth Amendment in the age of technology. Fortunately, a number of high-exposure uses of Stingrays, such as their use by the IRS and the revelation that the Baltimore police used airplane-borne cell tower simulators to monitor protest crowds, has ensured bipartisan interest in setting forth strong guidelines for their use.

It will be the task of lawmakers and civil liberties advocates to ensure that these guidelines are sufficient and that they do not continue to provide avenues for yet another form of legally justified, unconstitutional government mass surveillance.