GlobalResearch
Center for Research on Globalization

Stingray, the Cell Phone Spying Device: US Government "Disappears" Stingray Spying Records

By Peter Van Buren
Global Research, June 30, 2014
The Dissenter 21 June 2014

Region: USA
Theme: Intelligence, Law and Justice, Police State & Civil Rights

We've heard variations on the phrase "If you have nothing to hide, you have nothing to fear" from the government for quite some time. It appears this may be true, at least if you are the government.

In the case of Stingray, a cell phone spying device used against Americans, the government does have something to hide and they fear the release of more information. Meanwhile, the Fourth Amendment weeps quietly in the corner.

Stingray

Cell phone technology is very useful to the cops to locate you and to track your movements. In addition to whatever as-yet undisclosed things the NSA may be up to on its own, the FBI acknowledges a device called Stingray to create electronic, "fake," cell phone towers and track people via their phones in the U.S. without their knowledge. The tech does not require a phone's GPS. This technology was first known to have been deployed against America's enemies in Iraq, and it has come home to be used against a new enemy– you.

Stingray, also known as an International Mobile Subscriber Identity, or IMSI, catcher, works like this. The cell network is designed around triangulation and whenever possible your phone is in constant contact with at least three towers. As you move, one tower "hands off" your signal to the next one in your line of motion. Stingray electronically inserts itself into this process as if it was a (fake; "spoofed") cell tower itself to grab location data before passing your legitimate signal back to the real cell network. The handoffs in and out of Stingray are invisible to you. Stingrays also "inadvertently" scoop up the cell phone data of anyone within several kilometers of the designated target person. Though typically used to collect location metadata, Stingray can also capture conversations, texts and mobile web use if needed.

Stingray offers some unique advantages to a national security state: it bypasses the phone company entirely, which is handy if laws change and phone companies no longer must cooperate with the government, or simply if the cops don't want the phone company or anyone else to know they're snooping.

This has led the Electronic Frontier Foundation (EFF) to warn

> "A Stingray— which could potentially be beamed into all the houses in one neighborhood looking for a particular signal— is the digital version of the pre-Revolutionary war practice of British soldiers going door-to-door, searching Americans' homes without rationale or suspicion, let alone judicial approval...

[Stingray is] the biggest technological threat to cell phone privacy."

Trying to Learn about Stingray

Learning how Stingray works is difficult.

The Electronic Privacy Information Center filed a FOIA request for more information on Stingrays, but the FBI is sitting on 25,000 pages of documents explaining the device that it won't release.

The device itself is made by the Harris Corporation. Harris makes electronics for commercial use and is a significant defense contractor. For Stingray, available only to law enforcement agencies, Harris requires a non-disclosure agreement that police departments around the country have been signing for years explicitly prohibiting them from telling anyone, including other government bodies, about their use of the equipment "without the prior written consent of Harris."

A price list of Harris' spying technology, along with limited technical details, was leaked online, but that's about all we know.

Though the non-disclosure agreement includes an exception for "judicially mandated disclosures," there are no mechanisms for judges even to learn that the equipment was used at all, thus cutting off any possibility they could know enough demand disclosure. In at least one case in Florida, a police department revealed that it had decided not to seek a warrant to use the technology explicitly to avoid telling a judge about the equipment. It subsequently kept the information hidden from the defendant as well. The agreement with Harris goes further to require law enforcement to notify Harris any time journalists or anyone else files a public records request to obtain information about Stingray and also demands the police department assist Harris in deciding what information to release.

Something to Hide

An evolving situation in Florida shows how hard the government is working to keep the details of its Stingray spying on Americans secret.

The ACLU originally sought Stingray records in Sarasota, Florida after they learned a detective there obtained permission to use the device simply by filing an application with a local court, instead of obtaining a probable-cause warrant as once was required by the Fourth Amendment of the Constitution. It became clear that the Sarasota police had additionally used Stingray at least 200 times since 2010 without even the minimal step of even notifying a judge. In line with the non-disclosure agreement, very rarely were arrested persons advised that Stingray data was used to locate and prosecute them.

The ACLU, which earlier in 2014 filed a Florida state-level FOIA-type request with the Sarasota police department for information detailing its use of Stingray, had an appointment with the local cops to review documents. The local police agreed to the review. However, the June 2014 morning of the ACLU's appointment, U.S. Marshals arrived ahead of them and physically took possession of the files. The Marshals barred the Sarasota police from releasing them. The rationale used by the federal government was that having quickly deputized a Sarasota cop, all Sarasota records became federal property.

"This is consistent with what we've seen around the country with federal agencies trying to meddle with public requests for Stingray information," an ACLU spokesperson said, noting that federal authorities have in other cases invoked the Homeland Security Act to prevent the release of such records. "The feds are working very hard to block any release of this information to the public."

The Cops are Lying in Court about Stingray

Yeah, it gets worse. According to emails uncovered by the ACLU, Florida law enforcement had concealed the use of Stingray in court documents. Specifically, one e-mail from Sarasota police to North Port police states, "In reports or depositions we simply refer to the assistance as 'received information from a confidential source regarding the location of the suspect.' To date this has not been challenged." By hiding the fact from the court (and the defendant) that information used in the prosecution came from Stingray, the police effectively blocked any possibility that that information could be challenged in court. This appears in direct confrontation with the Sixth Amendment's right to confront witnesses.

Russell Covey, a law professor at Georgia State University, stated

> "The failure of law enforcement officials to disclose to courts the actual source of their information and to pretend that it came from a 'confidential source,' is deceptive and possibly fraudulent. Affirmatively misleading the courts about the source of evidence in sworn warrant applications would clearly constitute a constitutional violation."

A Court Says the Feds Can Hide the Records

Following the feds' seizure of the Stingray records, the ACLU filed an emergency motion with a Florida court that would require Sarasota to make its Stingray records available. However, in a decision issued June 17, 2014, a Florida state circuit court judge found that his court lacked jurisdiction over a federal agency, allowing the transfer of the Stingray documents to the feds and de facto blocking their release.

The ACLU plans further appeals. Unless and until they succeed, details of another way of spying on Americans will remain secret. The government does indeed have something to hide.

*Peter Van Buren writes about current events at blog. His book,*Ghosts of Tom Joad: A Story of the #99Percent, *is available now from from Amazon.*

Articles by: Peter Van Buren