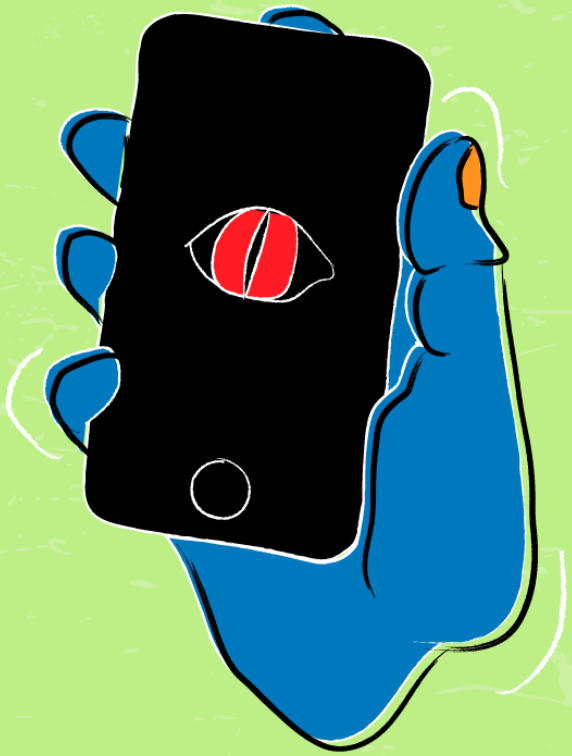

An Issue Brief on

# StingRays

RESTORE the FOURTH

## What are StingRays and how do they work?

Our phones have revolutionized our lives. Over 80% of Americans have a smartphone, and we use them for a thousand different things: communicating with friends and family, documenting our lives, finding our way, and reminding us of important events. They're as private as personal diaries—and like one, contain a true treasure trove of personal information. Many of us assume that if we put a passcode on our phone, the information stored on it is "secure." But that isn't necessarily true, and there's a police surveillance technology that proves that.

The specific surveillance technology we're referring to are called IMSI-catchers, commonly known as StingRays. Thsee are a type of surveillance tech that can gather information about us through our phones—without us even knowing it.

StingRays were initially developed for military and intelligence use, but since at least 1995, devices with these capabilities have been marketed to and have become popular with domestic law enforcement agencies. StingRay-type devices operate in two different ways; passive and active.

Passive IMSI-catchers work by "catching" (and eventually releasing) signals from your cell phone as they're being sent to a cell tower.

Active IMSI-catchers work by simulating a cell tower. These are often called Cell-Site Simulators. This works by taking advantage of the way cell phones are designed: cell phones automatically connect to the cell tower with the strongest signal in order to give you the best connection possible, so active IMSI-catchers put out a signal that is stronger than other cell towers in the area, tricking your phone into connecting to it.

StingRay-type devices collect a wide variety of data from your cellphone. All StingRay-type devices can be used to collect your ESN and IMSI numbers; numbers that are personally identifiable and can be traced back to your phone. StingRay-type devices are also often used to collect your location data. Certain types of IMSI-catchers can also collect unencrypted information such as websites you visit, calls, messages, and metadata such as when a call was made and how long it lasted. Some devices related to StingRays can even go a step further, and are able to perform denial of service attacks and eavesdrop on phone conversations. There are some concerns that StingRay-type devices can be used to inject malware into a target phone. In January 2020, journalists in Morocco suspected they had been targeted by a network injection attack carried out via an IMSI-catcher with this capability.

It's a common misconception that StingRays are large and require some sort of satellite-outfitted van. StingRays and their related devices are actually quite small and portable. They are commonly mounted in vehicles but can also be concealed in a briefcase or even handheld. When handheld, they are sometimes called "KingFish." More advanced IMSI-catchers are sometimes marketed under the name "Hailstorm." They can be used from low-flying aircraft or, as miniaturization advances, even from drones.

## Why should you be worried about StingRays?

Since the 90s, technologists have known that theoretically a device like a StingRay could exist, but they were first found to be used by police departments in a case involving Daniel Rigmaiden. Rigmaiden, who went by multiple aliases and was ruthless about privacy, had caught the attention of Baltimore PD after being suspected of committing fraud. Rigmaiden noticed that the search warrant for his apartment did not mention how law enforcement had come to know his identity. Research led Rigmaiden to uncovering Baltimore PD's use of a StingRay to track him down, leading to one of the first pieces of journalism revealing to the public the widespread, constitutionally-questionable use of StingRay devices.

While police departments cite counter-terrorism as justification for their purchases of StingRays and other IMSI-catchers, law enforcement commonly use StingRays in order to solve minor crimes. Reporting out of Baltimore shows that cops have used StingRays in thousands of cases, using the

devices more than 4,300 times over an eight-year period. Documents published by the ACLU show that police in Florida most commonly used StingRays for solving minor crimes; this means that police may be actively violating bystanders' constitutional rights in order to solve petty crimes such as theft.

StingRays are commonly discussed in relation to surveillance tech that is used on protesters. While there is not yet conclusive evidence that this happens, it is highly probable. In 2014, protesters in Chicago noticed their phones were not working properly when a police vehicle suspected of being outfitted with a StingRay was nearby. Contemporaneous police communications appeared to show their local fusion center was tracking cellphones within that same protest. While there are similar reports from protests across the country, their use on protestors has not yet been conclusively proven.

One reason we do not have conclusive evidence that StingRays are used on protesters is because it is almost impossible to prove their involvement without discovery materials relating to an actual criminal case—for example, a warrant referring to a StingRay being used. While it is likely, it's important to keep in mind that network disruptions caused by a StingRay can look quite similar to a non-StingRay network disruption.

**"Baltimore...cops have used StingRays in thousands of cases, using the devices more than 4,300 times over an eight-year period."**

While a warrant may offer some evidence that a StingRay has been used, police departments often conceal their usage of these devices through vague and euphemistic language when applying for a warrant—as seen in the Rigmaiden case. A police department in Florida admitted in emails to having used parallel construction in order to conceal that they had been using a StingRay-type device to gather evidence on a suspect. This is because often the manufacturers of StingRay-type devices—and sometimes even the FBI—require police departments to sign non-disclosure agreements in order to purchase and use StingRays. Federal law enforcement will often push for dismissal of cases if it becomes clear that going through with the case will reveal specifics about how IMSI-catchers are used and operate.

There have also been cases of ICE using StingRays to track down undocumented immigrants in order to arrest, imprison, and eventually deport them. As an additional barrier, ICE often doesn't disclose usage of this technology; which cloaks the use of IMSI-catchers in even more secrecy, interferes with the legal process, and prevents public oversight of these cases. Advocates have decried the use of StingRays in immigration cases as "excessive."

One major protest-related Fourth Amendment concern regarding StingRays is that, while law enforcement may be using it to target one individual's phone, they will inevitably be sweeping up large numbers of bystanders' data. Theoretically, police could then exploit that swept up data to find evidence of other suspicious activity. StingRays' access of cell site location information and other phone data in real-time also has Fourth Amendment implications.

In *Carpenter v. United States*, the Supreme Court declared that, when it comes to cell phone location data, "the Government's obligation is a familiar one—get a warrant." Regardless of this, the state of laws regarding StingRays is in flux. In 2015, the Attorney-General issued guidance that federal law enforcement agents would have to obtain a search warrant based on probable cause before using a StingRay, instead of the common prior practice of using "pen register" or "trap and trace" orders that do not require probable cause. Federal courts, beginning in 2016, have started to exclude the use of StingRay-derived evidence, but it is still common for state and local police to not specify on their warrant applications that a StingRay will be used, resulting in judges approving warrants without a full appreciation of what will be searched or seized. Consequently, state legislatures still need to pass laws requiring warrant protections, and the Attorney-General's guidelines need to be backed by a federal statute.

## What can be done about StingRay devices?

Theoretically, one can create a device that can "sniff out" IMSI-catchers. In order to create a device to find IMSI-catchers, you would need hardware like a BladeRF and open source code maintained by the EFF called "Crocodile Hunter." This tech can theoretically detect when a Hailstorm device (a more advanced form of IMSI-catcher) is being used on a cellphone by analyzing data that the phone reports about the cell tower (primarily the location of the cell tower or Hailstorm device) and comparing it against known data, like maps of legitimate cell towers.

There are also efforts to pass legislation regulating the use of StingRay-type devices. Restore the Fourth has been involved in a few efforts to get such legislation passed, both local and national. Some examples of regulation include requiring law enforcement to get a warrant that specifically mentions StingRay usage before deploying them.

## What has Restore the Fourth done to rein in StingRays?

We support the passing of local ordinances that increase public oversight of surveillance technology, including StingRay devices. Restore the Fourth has been a vital part of efforts to pass CCOPS and other surveillance oversight legislation in a variety of localities, including Boston. Restore The Fourth – Boston and RI-Rights have supported efforts in their state legislatures to require warrants before state and local law enforcement can deploy StingRays.

Restore the Fourth is currently involved in a bipartisan effort to get a national bill regulating StingRay use passed in Congress with the help of Representative Ted Lieu and Senator Ron Wyden with Senator Steve Daines and Representative Tom McClintock. This bill requires warrants for law-enforcement use of StingRay devices, and would require those warrants specifically mention StingRay usage—instead of the current common practice of vague warrants euphemistically alluding at usage of technological devices to gather evidence. This also requires that any StingRay use be disclosed to the defendants in a criminal case, an issue we've seen repeatedly come up with StingRay usage to gather evidence on a defendant (see, again, the Daniel Rigmaiden case). It also limits information that law enforcement are allowed to collect with StingRay devices to just identifying information, and gives public right of action to any individual affected by unlawful StingRay usage.

**You can read the full bill text here.**