WIRED

How the Government Hides Secret Surveillance Programs

Louise Matsakis
01/09/2018

In 2013, 18-year-old Tadrae McKenzie robbed a marijuana dealer for $130 worth of pot at a Taco Bell in Tallahassee, Florida. He and two friends had used BB guns to carry out the crime, which under Florida law constitutes robbery with a deadly weapon. McKenzie braced himself to serve the minimum four years in prison.

But in the end, a state judge offered McKenzie a startlingly lenient plea deal: He was ordered to serve only six months' probation, after pleading guilty to a second-degree misdemeanor. The remarkable deal was related to evidence McKenzie's defense team uncovered before the trial: Law enforcement had used a secret surveillance tool often called a Stingray to investigate his case.

Stingrays are devices that behave like fake cellphone towers, tricking phones into believing they're pinging genuine towers nearby. By using the device, cops can determine a suspect's precise location, outgoing and incoming calls, and even listen-in on a call or see the content of a text message.

Many people may have been convicted using techniques that violated their rights.

McKenzie's lawyers suspected cops had used a Stingray because they knew exactly where his house was, and knew he left his home at 6 a.m. the day he was arrested. The cops had obtained a court order from a judge to authorize Verizon to hand over data about the location of Mckenzie's phone. But cell tower data isn't precise enough to place a device at a specific house.

The cops also said they used a database that lets law enforcement agencies locate individuals by linking them with their phone numbers. But the phone McKenzie was using was a burner, and not associated with his name. Law enforcement couldn't adequately explain their extraordinary knowledge of his whereabouts.

The state judge in the case ordered police to show the Stingray and its data to McKenzie's attorneys. They refused, because of a non-disclosure agreement with the FBI. The state then offered McKenzie, as well as the two other defendants, plea deals designed to make the case go away.

The cops in McKenzie's case had ultimately failed to successfully carry out a troubling technique called "parallel construction."

First described in government documents obtained by Reuters in 2013, parallel construction is when law enforcement originally obtains evidence through a secret surveillance program, then tries to seek it out again, via normal procedure. In essence, law enforcement creates a parallel, alternative story for how it found information. That way, it can hide surveillance techniques from public scrutiny and would-be criminals.

A new report released by Human Rights Watch Tuesday, based in part on 95 relevant cases, indicates that law enforcement is using parallel construction regularly, though it's impossible to calculate exactly how often. It's extremely difficult for defendants to discern when evidence has been obtained via the practice, according to the report.

"When attorneys try to find out if there's some kind of undisclosed method that's been used, the prosecution will basically stonewall and try not to provide a definitive yes or no answer," says Sarah St. Vincent, the author of the report and a national security and surveillance researcher at Human Rights Watch.

In investigation reports, law enforcement will describe evidence obtained via secret surveillance programs in inscrutable terms. "We've seen plenty of examples where the police officers in those reports write 'we located the suspect based on information from a confidential source;' they use intentionally vague language," says Nathan Freed Wessler, a staff attorney at the ACLU's Speech, Privacy, and Technology project. "It sounds like a human informant or something else, not like a sophisticated surveillance device."

Sometimes, when a savvy defense attorney pushes, an unbelievable plea deal is offered, or the the case is dropped entirely. If a powerful, secret surveillance program is at stake, a single case is often deemed unimportant to the government.

"Parallel construction means you never know that a case could actually be the result of some constitutionally problematic practice," says St. Vincent. For example, the constitutionality of using a Stingray device without a warrant is still up for debate, according to the Human Rights Watch report. Some courts have ruled that the devices do in fact violate the Fourth Amendment.

Hemisphere, a massive telephone-call gathering operation revealed by *The New York Times* in 2013, is one of the most well-documented surveillance programs that government officials attempt to hide when they use parallel construction. The largely secret program provides police with access to a vast database containing call records going back to 1987. Billions of calls are added daily.

In order to create the program, the government forged a lucrative partnership with AT&T, which owns three-quarters of the US's landline switches and much of its wireless infrastructure. Even if you change your number, Hemisphere's sophisticated algorithms can connect you with you new line by examining calling patterns. The program also allows law enforcement to have temporary access to the location where you placed or received a call.

The Justice Department billed Hemisphere as a counter-narcotics tool, but the program has been used for everything from Medicaid fraud to murder investigations, according to documentation obtained in 2016 by The Daily Beast.

"What Hemisphere's capabilities allow it to do is to identify relationships and associations, and to build people's social webs," says Aaron Mackey, staff attorney at the Electronic Frontier Foundation (EFF). "It's highly likely that innocent people who are doing completely innocent things are getting swept up into this database."

The EFF filed Freedom of Information Act and Public Records Act requests in 2014 seeking info about Hemisphere, but the government only provided heavily redacted files. So the EFF filed a lawsuit in 2015. It's currently waiting for a California judge to decide whether more information can be made public without impeding law enforcement's work.

"[The government] is obscuring what we believe to be warrantless or otherwise unconstitutional surveillance techniques, and they're also jeopardizing a defendant's ability to obtain all the evidence that's relevant," says Mackey.

Parallel construction can also involve a simple event like a traffic stop. In these instances, local law enforcement follows a suspect and then pulls them over for a mundane reason, like failing to use a turn signal. While the stop is meant to look random, cops are often working on a tip they received from a federal agency like the DEA.

"Sometimes when tips come through, the federal authorities don't even tell the local authorities what they're looking for," says St. Vincent. The tip could be as simple as to watch out for a car at a specific place and time.

These stops are referred to as "wall off" or "whisper" stops, according to the Human Rights Watch report. In these instances, local law enforcement has to find probable cause for pulling the suspect over to avoid disclosing the tip. The tip is then never mentioned in court, and instead the beginning of the investigation is said to be the "random" stop.

The Human Rights Watch report concludes that Congress should pass legislation forbidding the use of parallel construction because it impedes on the right to a fair trial. Some representatives, like Republican Senator Rand Paul, have also called for banning the practice.

Opponents of parallel construction believe it should be outlawed because it prevents judges from doing their jobs. "It really gives a lot of power to the executive branch," says St. Vincent. "It cuts judges out of the role of deciding whether something was legally obtained."

One of the most concerning aspects of the practice is it shields government surveillance technology from public scrutiny. Stingrays, the cellphone-tracking device used in the Florida robbery case, have existed for years, but have only recently been disclosed to the public. Lawyers and legal scholars haven't yet conclusively decided whether their use without a warrant violates the Fourth Amendment, in part because so little is known about them. That means many people may have been convicted using technology that violated their rights.

In the future, if the government hides new surveillance technology like facial recognition, the public will be unable to discern if it's biased or faulty. Unless judges and citizens understand how surveillance techniques are used, we also can't evaluate their constitutionality.

The public needs to determine if hiding surveillance programs is something it's comfortable with at all. On one hand, keeping certain techniques secret likely helps authorities apprehend criminals. But if we don't know at least the basic contours of how a program works, it's hard to have any discussion at all.