



## **Local Police Working With FBI To Amass Citizen Cell Phone Data**

By Adam Bates

June 14, 2016

Given such widespread use, and such obvious and troubling privacy implications, one would expect to find a large body of court rulings on the constitutionality of warrantless StingRay surveillance. One would be mistaken.

Our cellular phones, the U.S. Supreme Court recently opined, contain “a digital record of nearly every aspect of [our] lives – from the mundane to the intimate.” Indeed, many of us use our cellphones to privately convey our love, our insecurities, our fears, our locations, and our most sensitive relationships.

Yet right now, across the United States, law enforcement agents have secret, unfettered access to all of it, and the government is trying to keep it that way.

It was recently revealed that the FBI has been colluding with the Oklahoma City Police Department to conceal the use of equipment capable of powerful, surreptitious, and constitutionally dubious cellphone surveillance. The device, known as a StingRay, operates by mimicking the signal of a cell tower. The StingRay puts out a boosted signal that muscles out the signals of legitimate cell towers and forces nearby phones to connect to the device.

Once your phone is connected, the operator of the device can triangulate your position, see the incoming and outgoing numbers, and by all indications intercept the actual content of your communications. Police often deploy StingRays without probable-cause warrants or, in some cases, court orders. Even when police seek warrants and orders, the federal government has coached them to mislead judges about precisely what they are being asked to authorize.

StingRay deployments have been confirmed in at least 24 states and the District of Columbia, and there is every reason to believe many of the remaining states possess them and simply haven’t been forced to disclose it. Different departments have different deployment policies, but cities such as Baltimore have admitted to deploying the devices in thousands of investigations.

Given such widespread use, and such obvious and troubling privacy implications, one would expect to find a large body of court rulings on the constitutionality of warrantless StingRay surveillance. One would be mistaken.

Notwithstanding a promising recent Maryland appellate court ruling that StingRay surveillance is unconstitutional without a warrant, police departments in the rest of the country remain generally free to use the devices in complete secrecy. Shockingly few cases have been reviewed by the courts, and judicial and legislative oversight of law enforcement StingRay use is virtually nonexistent as a result. That secrecy is by design.

When local police departments receive federal permission to operate StingRays, they are required to coordinate the terms of use with the FBI. The FBI, in turn, requires that law enforcement agencies agree to an exhaustive list of conditions in order to acquire the device.

One of these terms, discovered only after a litigious freedom-of-information request by the New York Civil Liberties Union, explicitly forbids law enforcement and prosecutors from disclosing information about StingRay capability or use. The prohibition even applies to judges and defense attorneys, leaving the typical checks on police misconduct in the dark.

The agreement even allows the FBI to force state prosecutors to drop evidence or entire cases rather than reveal the use of StingRay surveillance. And that condition isn't hypothetical; it has actually happened around the country, resulting in dangerous criminals being let go or given sweetheart plea deals in order to maintain secrecy.

The agreement in the Oklahoma case is alarming because it goes even a step further. Rather than merely order the Oklahoma City Police Department not to disclose information regarding StingRay use, the memorandum tells the department to construct an entirely independent investigation around the "lead" created by the StingRay to obfuscate the source of the evidence.

In legal circles, this practice is known as "parallel construction," and it is particularly effective at concealing government investigative methods as well as government misconduct. In a parallel construction, the government uses evidence produced through confidential (or improper) means to create a new, seemingly independent investigation of illegal activity.

For instance, an illegal search of a target's trash could reveal the time and location of a future drug deal. A police officer could then follow the target on the night of the meeting and use any number of pretextual traffic violations to justify a stop and dog sniff of the car. When the drugs are discovered and the case goes to court, the government behaves as if it were the random traffic stop, and not the illegal search, that led to the arrest.

This "evidence-laundering" tactic conceals evidence from the court and from the defense, and as of September 2014, the FBI was explicitly counseling the Oklahoma City Police Department to use parallel construction to cover up its use of StingRay surveillance.

This deceit makes it difficult, if not impossible, for defendants to challenge the legality of the surveillance. Combined with the nondisclosure terms, parallel construction helps explain why

there has been so little judicial oversight of StingRay use despite thousands of deployments across the country.

Government surveillance techniques will continue to advance with the pace of technology. If the Fourth Amendment and the concept of individual privacy are to have any meaning at all moving forward, the judicial and legislative branches of government must take a stronger interest in protecting our constitutional rights against unfettered government access to the most intimate details and communications of our lives.

*Adam Bates is a policy analyst with the Cato Institute's Project on Criminal Justice. [abates@cato.org](mailto:abates@cato.org)*