The police are secretly using fake cellphone towers to spy on people

By Timothy B. Lee

April 22, 2015

Did you know that law enforcement can track your cellphone with a fake cell tower? It's true — and devices that do this, known as stingrays, are at the center of a growing scandal.

The FBI has done everything it could to keep the existence and use of stingrays a secret. Local law enforcement agencies are forced to sign nondisclosure agreements before they can use the devices. The FBI claims that revealing details about how the gadgets work would tip off criminals and terrorists, rendering them less effective.

But in recent months, civil liberties groups have steadily chipped away at the secrecy of these devices. We've learned that they're used by dozens — and probably hundreds — of law enforcement agencies across the country, and that at least one agency has used them thousands of times.

Critics say the way these devices have been used violates the US Constitution, by tracking people's locations without judicial oversight. And the secrecy surrounding the devices also appears to be hampering efforts to prosecute violent criminals, as prosecutors have dropped key evidence rather than discuss how it was obtained.

The extreme secrecy surrounding these devices is out of step with the American tradition of open and accountable government. Americans have a right to know that law enforcement spying has proper judicial oversight. And this kind of oversight is impossible if even basic information about the technology is kept under wraps.

Stingrays are fake cellphone towers police use to spy on people

When you turn on your cellphone, it scans the surrounding area to find the cellular tower with the best connection. It then communicates with this tower to send and receive phone calls and other data.

A device called a cell-site simulator, popularly known as a "stingray," lets law enforcement spy on people by pretending to be a cellphone tower. This device, not much larger than a toaster, fools nearby mobile devices into connecting to it instead of to a real cellphone tower. That gives law enforcement information about the identity and precise location of nearby mobile devices. Police departments say they never use the devices to intercept the contents of people's calls or messages, though it's hard to verify that without knowing more about how they work.

By turning everyone's cellphone into a tracking device, stingrays allow cops to track suspects from the back of a van hundreds of feet away — without any help from the target's cellular provider. Unsurprisingly, the devices have proliferated to police departments across the country.

And while we don't know the full extent of Stingray use, there's evidence that they're used heavily by law enforcement agencies. The ACLU has compiled a map of states where law enforcement is known to be using the devices — there are almost certainly other places where their use has yet to be uncovered:

How often are the devices used? Most police departments won't say. But police in Baltimore recently admitted that they've used the device 4,300 times. And we don't know how many of these uses occurred with court approval — we'll discuss the legal issues more below.

The FBI has closely guarded the secrecy of stingray technology

We know that many law enforcement agencies use this technology, but we don't know how many agencies use the devices or how often they do so. That's because an elaborate scheme has mostly kept the devices out of the public eye until recently.

Because stingrays emit radio waves, they must be approved by the Federal Communications Commission before they can be used. Harris Corporation, the leading manufacturer of the devices, asked the FCC to require state and local law enforcement agencies to get approval from the FBI before they can use the devices. And the FBI, in turn, requires law enforcement agencies to sign nondisclosure agreements in order to get access.

The FBI declined to comment for this story, but a spokesman sent me a copy of a 2014 affidavit from an FBI official explaining why the agency requires that information about the devices be kept secret. The FBI says that giving the public details about how stingray technology works or how it's used could provide criminals and terrorists with information that allows them to "develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to thwart the use of this technology."

The FBI thinks that releasing even seemingly minor information can cause harm, since the bad guys can piece together different bits of information to learn how stingrays work and how they can be evaded.

Earlier this month, the New York Civil Liberties Union obtained a copy of the nondisclosure agreement the FBI asked the sheriff's office in Erie County, New York, to sign in order to use cell-site simulators. The agreement bars recipients from telling anyone about the devices, and specifically prohibits Erie County law enforcement from disclosing information about stingray technology in court.

Stingray secrecy appears to be hampering prosecutions

The FBI's gag order appears to be undermining efforts to prosecute violent criminals. This week, for example, the St. Louis Post-Dispatch reported that the St. Louis city police chose to drop the prosecution of three men charged in a violent robbery spree shortly before a government witness would have had to testify about the use of stingray devices in the case. Prosecutors say the timing was a coincidence.

In a Baltimore case last year, prosecutors chose to drop evidence about the location of a suspect's phone after an angry judge insisted that police explain how they had located it. In Florida, prosecutors offered a defendant a generous plea deal to avoid having to comply with a judge's order to show a stingray device to the defendants' lawyers.

If the FBI continues insisting on keeping the devices secret, this problem is only going to get worse. In the past, defense attorneys didn't know that stingrays existed, so they didn't ask questions about them. But now defense lawyers not only know the devices exist, they also know that pressing for information about them can force prosecutors to drop the case. So expect law enforcement to face a lot more awkward questions about this in the coming months.

Meanwhile, there are signs that judges are getting fed up with the secrecy surrounding stingrays. When a Baltimore police officer said he was barred from discussing the stingray in court due to a nondisclosure agreement, Baltimore Judge Barry Williams retorted, "You don't have a nondisclosure agreement with the court," and threatened to hold the cop in contempt if he didn't answer the question.

Stingrays — and stingray secrecy — raise constitutional issues

Adam Bates, an analyst at the Cato Institute (where I was a staff writer from 2003 to 2005), says that law enforcement use of stingrays raises two different constitutional issues.

One has to do with the Fourth Amendment. While the law isn't totally clear, a 2012 Supreme Court ruling suggested that tracking a suspect's location without a warrant may run afoul of the Fourth Amendment's rule against warrantless surveillance. For example, Bates notes that documents in Erie County showed that police "had deployed the device 47 times and had only gotten one court order." Future court cases will likely clarify when the police must seek judicial approval before tracking suspects.

A related problem, Bates says, is that when police use a stingray, they capture information about every cellphone in a large area. That means that in the process of spying on a single criminal suspect, they may also capture information about the location of dozens of totally innocent people, as well — making judicial oversight all the more necessary.

Also, it wouldn't be difficult for stingray-type devices to intercept not only a suspect's location and identity, but also the contents of his communications. Bates says law enforcement agencies have consistently denied that they do this. But given the potential for abuse, he argues that more oversight is needed to verify that these devices are not being used for illegal wiretapping.

And Bates says the FBI's gag order raises additional constitutional issues. "We have a long history of not allowing that kind of secret evidence," Bates says. The Constitution guarantees defendants the right to see evidence used against them and interrogate opposing witnesses. So even if warrantless stingray surveillance is legal, barring prosecutors and police officers from discussing it in court might still violate the Constitution.

It's time for the FBI to come clean about stingrays

The FBI claims it needs to keep information about stingrays under wraps to prevent the bad guys from learning how to evade surveillance. That argument might have made sense a decade ago when the use of this technology was unknown, but it doesn't make much sense today.

This isn't how we handle other police surveillance techniques. For example, law enforcement has long had the power to wiretap people's telephones. Information about specific wiretapping operations — whose phone lines are being tapped, and when — are kept secret for obvious reasons. But the existence of wiretapping capabilities is not a secret.

Nevertheless, criminals regularly make incriminating statements over tapped phone lines. That's partly because criminals can be careless, and partly because it's hard to know which information might turn out to be incriminating. There's no reason to think that providing more information about how stingrays work would destroy the devices' utility to law enforcement.

We don't know if warrantless cellphone tracking is legal or not. Law enforcement agencies have insisted that the Fourth Amendment doesn't apply in this type of situation, and the courts have yet to squarely address the situation. Prosecuting people using secret evidence certainly seems constitutionally problematic.

In any event, there's no way to put the stingray genie back in the bottle. At this point, smart criminals are going to assume that the police have the ability to track their cell phones. If the FBI continues to insist on secrecy, it's only going to hamper the efforts of prosecutors, who will be put at a disadvantage by their inability to explain how they got incriminating evidence.