WASHINGTON Examiner

Cellphone spying unchecked, say experts

Rudy Takala
September 14, 2015

The Justice Department issued new guidelines governing the use of "Stingray" phone surveillance technology by federal agencies this month. The rules are intended to assuage concerns that the technology is being used to engage in widespread, warrantless spying on Americans. However, critics say the guidelines lack real substance.

The reason for that is threefold. First is that they apply only to federal agencies under Justice, not state or local law enforcement. Second, while they require warrants in some circumstances, they allow for exceptions in others. Third, they are not legally binding.

"The impact remains to be seen," said Adam Bates, a policy analyst for the Cato Institute. "There are a lot of exceptions to the warrant requirement. For instance, one cited exception is the prevention of escape by a suspect or convicted fugitive. That's pretty much the entire job description of the U.S. Marshals Service. So it's unlikely that the new policy will have an effect there."

Stingray technology simulates cellphone towers, allowing cellphones in a given area to connect to them. In order to search for a single suspect, the technology vacuums up information from hundreds or thousands of phones in an area. The Justice Department claims it doesn't collect the content of communications, even though it has the ability to do so. It is meant only to collect metadata, which includes a cellphone user's location and the identities of those they communicate with.

In a recent analysis of what precisely that means, one ABC reporter, Will Ockenden, requested six months of his metadata records from his telephone company. In response, he received 1,500 instances of calls and text messages that he had made and 11,200 instances of "data sessions," or occasions on which his phone connected to the Internet over his mobile network. From the data, it was possible to extrapolate where he lived, worked, how he traveled, and where he spent his time.

Proponents of the technology argue that telephone users do not "own" their metadata, and as such, have no right to expect that it be kept private. Nate Cardozo, a staff attorney for the Electronic Frontier Foundation, disagrees.

"The argument that metadata deserves less protection than content has no merit in the 21st century," Cardozo told the *Washington Examiner*. "Metadata provides enough context to know some of the most intimate details of your lives. Metadata is key to privacy."

Additionally, even if the technology has occasionally been used to go beyond the collection of metadata and captured the actual content of communications, law enforcement has no obligation to disclose it. If, for instance, a rogue officer used it for that purpose at the local level, his agency would be legally prevented from disclosing the misuse under the terms of the non-disclosure agreements they sign with Justice.

"It's not credible that law enforcement has never used a feature included on devices specifically designed for law enforcement," Cardozo said. Some members of Congress have had similar suspicions. Three letters of inquiry sent by Sens. Chuck Grassley, R-Iowa, and Patrick Leahy, D-Vt., have failed to yield a public response to that question.

While the new guidance are intended to apply to agencies like the DEA, FBI and ATF, it does not apply to local agencies. Through press reports and Freedom of Information Act requests, law enforcement units in more than 20 states have been identified as using Stingray devices. More likely exist.

Advocates say the secrecy is necessary to protect national security. Others, such as Bates, have said that argument doesn't make sense.

"We know from FOIA efforts that these devices in state and local hands are virtually always used for routine law enforcement actions that have nothing to do with national security," Bates said. "Certainly drug traffickers and terrorists figured out long ago that their cellphones were a liability. That's no justification for these devices, which can and do sweep up troves of data from innocent people not suspected of any crime. The usual defense that secrecy is a requirement for the effective use of this technology is unacceptable."

Cardozo feels similarly, advocating for more concrete privacy protections. "Without a statute or court decision giving this voluntary policy the force of law, there's nothing keeping warrantless Stingray evidence out of court, and therefore nothing to deter agents from behaving badly."

"It's nice to have an admission of these devices being used," Bates added, "and it's nice to have a written commitment to the warrant requirement, but there are a lot of big gaps in that warrant requirement, and state and local Stingray use appears to be continuing unabated."