The New York Times | http://nyti.ms/1GaPGZu

TECHNOLOGY

A Police Gadget Tracks Phones? Shhh! It's Secret

By MATT RICHTEL MARCH 15, 2015

A powerful new surveillance tool being adopted by police departments across the country comes with an unusual requirement: To buy it, law enforcement officials must sign a nondisclosure agreement preventing them from saying almost anything about the technology.

Any disclosure about the technology, which tracks cellphones and is often called StingRay, could allow criminals and terrorists to circumvent it, the F.B.I. has said in an affidavit. But the tool is adopted in such secrecy that communities are not always sure what they are buying or whether the technology could raise serious privacy concerns.

The confidentiality has elevated the stakes in a longstanding debate about the public disclosure of government practices versus law enforcement's desire to keep its methods confidential. While companies routinely require nondisclosure agreements for technical products, legal experts say these agreements raise questions and are unusual given the privacy and even constitutional issues at stake.

"It might be a totally legitimate business interest, or maybe they're trying to keep people from realizing there are bigger privacy problems," said Orin S. Kerr, a privacy law expert at George Washington University. "What's the secret that they're trying to hide?"

The issue led to a public dispute three weeks ago in Silicon Valley, where a sheriff asked county officials to spend $502,000 on the technology. The Santa Clara County sheriff, Laurie Smith, said the technology allowed for locating cellphones — belonging to, say, terrorists or a missing person. But when asked for details, she offered no technical specifications and acknowledged she had not seen a product demonstration.

Buying the technology, she said, required the signing of a nondisclosure agreement.

"So, just to be clear," Joe Simitian, a county supervisor, said, "we are being asked to spend $500,000 of taxpayers' money and $42,000 a year thereafter for a product for the name brand which we are not sure of, a product we have not seen, a demonstration we don't have, and we have a nondisclosure requirement as a precondition. You want us to vote and spend money," he continued, but "you can't tell us more about it."

The technology goes by various names, including StingRay, KingFish or, generically, cell site simulator. It is a rectangular device, small enough to fit into a suitcase, that intercepts a cellphone signal by acting like a cellphone tower.

The technology can also capture texts, calls, emails and other data, and prosecutors have received court approval to use it for such purposes.

Cell site simulators are catching on while law enforcement officials are adding other digital tools, like video cameras, license-plate readers, drones, programs that scan billions of phone records and gunshot detection sensors. Some of those tools have invited resistance from municipalities and legislators on privacy grounds.

The nondisclosure agreements for the cell site simulators are overseen by the Federal Bureau of Investigation and typically involve the Harris Corporation, a multibillion-dollar defense contractor and a maker of the technology. What has opponents particularly concerned about StingRay is that the technology, unlike other phone surveillance methods, can also scan all the cellphones in the area where it is being used, not just the target phone.

"It's scanning the area. What is the government doing with that information?" said Linda Lye, a lawyer for the American Civil Liberties Union of Northern California, which in 2013 sued the Justice Department to force it to disclose more about the technology. In November, in a response to the lawsuit, the government said it had asked the courts to allow the technology to capture content, not just identify subscriber location.

The nondisclosure agreements make it hard to know how widely the technology has been adopted. But news reports from around the country indicate use by local and state police agencies stretching from Los Angeles to Wisconsin to New York, where the state police use it. Some departments have used it for several years. Money for the devices comes from individual agencies and sometimes, as in the case of Santa Clara County, from the federal government through Homeland Security grants.

Christopher Allen, an F.B.I. spokesman, said "location information is a vital component" of law enforcement. The agency, he said, "does not keep repositories of cell tower data for any purpose other than in connection with a specific investigation."

A fuller explanation of the F.B.I.'s position is provided in two publicly sworn affidavits about StingRay, including one filed in 2014 in Virginia. In the affidavit, a supervisory special agent, Bradley S. Morrison, said disclosure of the technology's specifications would let criminals, including terrorists, "thwart the use of this technology."

"Disclosure of even minor details" could harm law enforcement, he said, by letting "adversaries" put together the pieces of the technology like assembling a "jigsaw puzzle." He said the F.B.I. had entered into the nondisclosure agreements with local authorities for those reasons. In addition, he said, the technology is related to homeland security and is therefore subject to federal control.

In a second affidavit, given in 2011, the same special agent acknowledged that the device could gather identifying information from phones of bystanders. Such data "from all wireless devices in the immediate area of the F.B.I. device that subscribe to a particular provider may be incidentally recorded, including those of innocent, nontarget devices."

But, he added, that information is purged to ensure privacy rights.

In December, two senators, Patrick J. Leahy and Charles E. Grassley, sent a letter expressing concerns about the scope of the F.B.I.'s StingRay use to Eric H. Holder Jr., the attorney general, and Jeh Johnson, the secretary of Homeland Security.

The Harris Corporation declined to comment, according to Jim Burke, a company spokesman. Harris, based in Melbourne, Fla., has $5 billion in annual sales and specializes in communications technology, including battlefield radios.

Jon Michaels, a law professor at the University of California, Los Angeles, who studies government procurement, said Harris's role with the nondisclosure agreements gave the company tremendous power over privacy policies in the public arena.

"This is like the privatization of a legal regime," he said. Referring to Harris, he said: "They get to call the shots."

For instance, in Tucson, a journalist asking the Police Department about its StingRay use was given a copy of a nondisclosure agreement. "The City of Tucson

shall not discuss, publish, release or disclose any information pertaining to the product," it read, and then noted: "Without the prior written consent of Harris."

The secrecy appears to have unintended consequences. A recent article in The Washington Post detailed how a man in Florida who was accused of armed robbery was located using StingRay.

As the case proceeded, a defense lawyer asked the police to explain how the technology worked. The police and prosecutors declined to produce the machine and, rather than meet a judge's order that they do so, the state gave the defendant a plea bargain for petty theft.

At the meeting in Santa Clara County last month, the county supervisors voted 4 to 1 to authorize the purchase, but they also voted to require the adoption of a privacy policy.

(Sheriff Smith argued to the supervisors that she had adequately explained the technology and said she resented that Mr. Simitian's questioning seemed to "suggest we are not mindful of people's rights and the Constitution.")

A few days later, the county asked Harris for a demonstration open to county supervisors. The company refused, Mr. Simitian said, noting that "only people with badges" would be permitted. Further, he said, the company declined to provide a copy of the nondisclosure agreement — at least until after the demonstration.

"Not only is there a nondisclosure agreement, for the time being, at least, we can't even see the nondisclosure agreement," Mr. Simitian said. "We may be able to see it later, I don't know."

A version of this article appears in print on March 16, 2015, on page A1 of the New York edition with the headline: A Police Gadget Tracks Phones? Shhh! It's Secret.