Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Lambis Case And The Future Of 'Stingray' Evidence

Law360, New York (August 19, 2016, 5:21 PM ET) --

Abraham J. Rein

In July, for the first time, a federal judge suppressed evidence in a criminal case from a device which, by mimicking a cell tower, can be used to geolocate a cellphone with surprising precision. The device is a cell-site simulator, often referred to as a "stingray." Versions of the stingray have been used by federal law enforcement since at least the 1990s, and controversy has swirled around the device since a government-imposed veil of secrecy began to lift earlier this decade. Where does the recent federal decision fit in this history, and what might its impact be? Let's begin with the case.

United States v. Lambis

In 2015, as part of an investigation into an international drug-trafficking organization, the U.S. Drug Enforcement Administration sought a warrant for information about the numbers dialed from a particular cellphone ("pen register data"), and for information about the phone's approximate location. The latter — approximate location information, often referred to as "cell site location information" (CSLI) — can be obtained from a cell service provider by compiling a record of "pings" sent to cell sites by the phone.

The CSLI made it possible for the DEA to locate the phone, which it believed belonged to a participant in the cocaine distribution conspiracy, "in the general vicinity" of "the Washington Heights area by 177th and Broadway." More precise location information was required; for this, the government needed the stingray.

"Stingray" is a generic term that refers to any of a number of devices that mimic cell towers for surveillance purposes. These devices can be used to locate a cellphone — in some cases to within two meters — by causing all nearby phones to connect to the device, identifying the devices, and measuring the relative strength of the signals. If the operator knows the phone's unique identifier, that phone's signals can be followed to a precise location. Stingray-type devices can also be used to identify the telephone numbers associated with all nearby phones, a technique sometimes used by law enforcement to figure out a suspect's phone number, or to determine his or her phone identifier for further tracking. And more sophisticated stingray devices can be used to intercept voice communications, selectively disable nearby phones, or even plant malware.

Notwithstanding that its warrant, which authorized the collection of pen register data and CSLI, did not expressly allow the use of a stingray, the government agents in the Lambis case used the device to track

the phone to a particular apartment building. Then they walked the halls of the building with the stingray and determined which apartment the phone was in. Later that night, agents returned to the apartment, knocked and obtained consent to enter the apartment; finding the suspect in his bedroom, they searched the room, where they uncovered digital scales, ziplock bags and 1,005 grams of cocaine.

The defendant argued that all of that evidence should be excluded, because the agents did not have a warrant to use the Stingray that led to the discovery. The Southern District of New York agreed. The court, relying on the Supreme Court's holding in Kyllo v. United States[1] — which found that police need a warrant to use thermal-imaging equipment to detect a marijuana-growing operation inside a home — found that this use of a stingray constitutes a "search" within the meaning of the Fourth Amendment, and therefore required a warrant (absent certain exceptions). Quoting Kyllo, the Lambis court explained: "Where ... the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[2]

As a result, the evidence located in the defendant's bedroom was "fruit of the poisonous tree" — evidence that would never have been found were it not for the tainted search — and had to be thrown out.

A Growing List of Attempts to Constrain Stingray Use

The Lambis case is part of a larger story of mounting attempts to constrain the government's use of stingrays, a technology whose use by law enforcement was largely unknown to the public as recently as 2011. Indeed, the government made efforts to keep information about the technology under wraps — local law enforcement agencies, for example, were required to execute non-disclosure agreements, prohibiting disclosure of any information about the devices under almost any circumstances, including sometimes providing that agencies must, "at the request of the FBI, seek dismissal of [a] case in lieu of using or providing, or allowing others to use or provide, any information concerning [the technology]" in the investigation.

Law enforcement agents who sought judicial permission to use cellular phone surveillance technology, as in the Lambis case, often were less than explicit about the particular technology they intended to use. One magistrate complained in 2013 that "what [federal agents] do is present an application that looks essentially like a pen register application ... So any magistrate judge that is typically looking at a lot of pen register applications and not paying a lot of attention to the details may be signing an application that is authorizing a stingray." A state court judge in Maryland speculated that the nondisclosure agreement itself was driving law enforcement's frequent reticence in applications for judicial permission to use the technology.

But in recent years, restrictions on government use of the technology have begun to emerge. On July 12, 2016, Rhode Island passed a bill requiring state agencies to obtain a warrant before seeking any "information concerning the location of an electronic device that, in whole or in part, is generated by or derived from the operations of that device" — language that would seem to cover the use of a stingray to locate a phone. A few days later, Rhode Island was joined by Illinois, which passed its own, arguably more comprehensive, Citizen Privacy Protection Act — a statute that requires a warrant before using the stingray's location capabilities, explicitly provides for an exclusionary remedy if the warrant requirement is violated, and outright prohibits using the device to intercept communications or disable phones, among other things. (Several other state statutes also require warrants for stingray use.) Illinois' legislature may have been reacting to an order issued by a Northern District of Illinois magistrate judge

in late 2015, which imposed several restrictions of the government's use of stingrays, including that officers must "make reasonable efforts" to minimize the number of innocent third parties' data that is swept up with each use, and that such third-party data must be "immediately" destroyed.

The Department of Justice itself also updated its policy in September 2015 to require — absent exigency or other unusual circumstances — that federal agents seek a warrant before using a stingray-type device. The Department of Homeland Security released its own, similar requirements for stingray usage a month later.

Most recently, controversy has erupted over a concern that law enforcement has been using reserved radio frequencies to operate the devices without seeking licenses required by the Federal Communications Commission. This concern prompted civil liberties groups to file a complaint with the FCC on Aug. 15, 2016, seeking a probe into the issue, and highlighting what may be a race-related disparity in the devices' use. The complaint makes the additional point that stingray-type devices can disrupt regular cellphone service — including that of innocent third parties who happen to be in the vicinity — potentially running afoul of strictly enforced FCC rules that prohibit wireless "blocking."

Potential Impact Going Forward

How might these constraints, and particularly the recent Lambis decision, have effects on stingray usage going forward? The answer to that question may vary between future cases and currently pending ones in which stingray evidence was used without an express warrant.

Future cases. Going forward, assuming the warrant requirement becomes standard (which is not necessarily a given — in 2013, the District of Arizona declined to exclude stingray evidence obtained with a warrant that was not explicit as to the technology to be used), a judicial official would have to agree with the government that probable cause supports the use of a Stingray before it can be used. Given the fact that, in many cases, the government has successfully obtained a warrant for CSLI, it seems likely that judges in future cases will be willing to extend permission to collect stingray data as well, which many may see as just another flavor of the same evidence-collection technique.

That said, there are important factors that distinguish stingray use from CSLI, which could give judges pause about issuing warrants. For one, use of a stingray can involve collecting data regarding the phones of any number of uninvolved third parties who happen to be in the vicinity. That data would include the phone's unique identifier, and can include other sensitive information, such as information about calls placed or received during the surveillance. Additionally, as illustrated by the arc of the Lambis investigation, stingrays have the capacity to geolocate a phone with much greater precision than CSLI arguably making it possible to track a subject's movements from room to room in a home, for example. For these reasons, stingray surveillance has the potential to be far more intrusive than CSLI. This could lead members of the judiciary who are educated about these nuances to think twice about granting a stingray warrant.

Pending cases. Given the reticence to reveal details about stingray surveillance, even in search warrant applications, it is likely that there are a large number of cases in a similar posture to Lambis — cases where a warrant was granted for CSLI and pen register data, but stingray data was collected. If other courts follow Lambis, are all of those cases at risk?

Some of those cases may well be affected by Lambis-type reasoning. Many others, however, will likely be factually distinguishable. The exclusionary rule is subject to a multitude of exceptions and

workarounds. In one, where officers "act with an objectively reasonable good-faith belief that their conduct is lawful," the evidence will not be excluded, even in the face of an unreasonable, warrantless search. This "good faith exception" was invoked in the first well-known stingray opinion, in which the magistrate explained that "a presumption of good faith attaches to searches conducted pursuant to a warrant." Because the officers relied on a warrant, albeit one that did not expressly permit stingray use, good faith was established, and the evidence was not excluded. Other courts may be inclined to follow similar reasoning.

Other exceptions to the exclusionary rule include the exigency exception — which can allow for warrantless searches under exigent circumstances, such as when necessary to prevent the imminent destruction of evidence or prevent a suspect's escape — and a rule that allows officers to perform a "protective sweep" of an area when arresting a suspect, to determine of potentially dangerous individuals are nearby. And under the "attenuation," "inevitable discovery," and "independent source" doctrines, evidence discovered in cases where an unauthorized stingray was used may nevertheless be admissible if the government can show a disconnect between the stingray's use and the evidence sought to be admitted.

One can imagine any of these doctrines saving warrantless stingray evidence in a large number of cases, particularly where courts are reluctant to set potentially guilty defendants — maybe large numbers of them — free over a widespread, if erroneous, government evidence-collection practice.

Conclusion

Stingray-type devices are extremely powerful. As with so many powerful new surveillance technologies, that means they have the potential to crack a lot of cases; it also means they have the potential to intrude on the privacy of a lot of innocent people. We are witnessing a society attempting to find the correct balance between those poles, and the Lambis case is one important piece of that undertaking. The project, however, continues — and the outcome will be shaped largely by the decisions of judges, magistrates and law enforcement in the coming months.

—By Abraham J. Rein, Post & Schell PC

Abraham Rein is an associate in Post & Schell's Philadelphia office and the co-chair of Post & Schell's information privacy & security practice group. He was also part of the team that won the Facebook speech case, United States v. Elonis, in the Supreme Court of the United States.

[1] 533 U.S. 27, 33 (2001).

[2] Kyllo, 533 U.S. at 40.
