IPhone Access Gets Attention, 'Stingrays' Fly Under The Radar

Written by Erik L. Schulwolf

April 6, 2016

Previously published in Law360, April 5, 2016. Posted with permission.

While eyes have been peeled on the U.S. Department of Justice's efforts to obtain a court order to hack the iPhone of one of the San Bernardino killers, garnering far less scrutiny is law enforcement's more routine use of powerful cellular tracking devices before a defendant is even charged. Called cell-site simulators, IMSI-catchers or "Stingrays" after the brand name of the leading product in the field, these trackers pose as a cell tower despite being the size of a suitcase, and can locate a cellphone within a matter of yards. These devices have caught the attention of privacy advocates and lawmakers because they can transmit the whereabouts of all other cellphones in the vicinity and are also capable of recording numbers of a phone's incoming and outgoing calls as well as intercepting the content of voice and text communications — information associated with innocent third parties.

What Do Courts Say About Law Enforcement's Use of Stingrays?

While there is limited federal case law pertaining to the use of Stingrays by law enforcement,[1] research has revealed recent cases addressing law enforcement's use of Stingrays that indicate that a search warrant (supported by probable cause) is required. See United States v. Rigmaiden, 2013 U.S. Dist. LEXIS 65633, at *43 – 45 (D. Ariz. May 8, 2013); In re United States, 2015 U.S. Dist. LEXIS 151811, at *9 – 10 (N.D.Ill. Nov. 9, 2015); In re United States, C.A. No. C-12-534M (S.D. Tex., Jun. 2, 2012).[2]

Although they both uphold the need for a search warrant, the District of Arizona in Rigmaiden and the Northern District of Illinois in In re United States take different approaches as to whether law enforcement must specifically disclose in a warrant application whether they will obtain information of unrelated third parties in the course of their investigation and their plans for protecting the privacy interests of those third parties.

In Rigmaiden, the District of Arizona concluded that the government's failure either to disclose in its warrant application that the Stingray would capture third party information, or to represent that the government would not use such third party information, did not require suppression. The court described the information about the Stingray's capture of third-party data as "a detail of execution which need not be specified" because the agents neither intended to collect nor used the third-party data collected by the Stingray, and because the warrant required the government to "expunge all of the data" collected by the Stingray at the end of the tracking mission.[3]

In contrast, the Northern District of Illinois held that a warrant seeking permission to use a Stingray must specifically include a provision directing law enforcement to minimize capture of third-party cellular signals, quickly destroy data other than those identifying the target's cellphone, and not use any data beyond those needed to ascertain the cellphone being used by the target.[4]

What Policies Impact Law Enforcement's Use of Stingrays?

Beyond case law, in recent months the DOJ and the U.S. Department of Homeland Security have put in place somewhat detailed policies on the legal processes that must be followed in order for law enforcement to use cell-site simulators.[5] Since September 2015, under DOJ policy, law enforcement agencies must obtain a search warrant supported by probable cause and issued under Rule 41 of the Federal Rules of Criminal Procedure in order to use a Stingray.[6] Authority under the Pen Register Statute, 18 USC § 3121 et seq., is also required.[7] The guidance lays out two exceptions to the warrant requirement. The first arises when there are exigent circumstances such that "the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable" under the Fourth Amendment.[8] Exigent circumstances include protecting human life or averting serious injury, preventing imminent destruction of evidence, hot

pursuit of a fleeing felon, and preventing the escape of a suspect or convicted fugitive.[9] The second arises when there are "other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable."[10]

Can Non-Law Enforcement Use Stingrays Too?

More concerning, perhaps, than the use of Stingrays by law enforcement is "the democratization of cellular interception technology."[11] While in the past, the high price for Stingray technology made purchase by non-law enforcement prohibitive, "[t]his cost barrier no longer exists."[12] There is evidence to support this assertion. As far back as 2010, a security researcher created a homemade Stringray-like device for $1,500.[13] A 2014 investigation by the Washington Post that used specially equipped cellphones "detected signs of as many as 18 [Stingray-like devices] in less than two days of driving through the [Washington, D.C.] region."[14]

While it is not clear to what extent there is — or will be — large-scale civilian use of Stingrays, the threat of such use underscores the need for the general public to be aware of the potential danger posed by Stingray-like devices, and for cellphone makers, cellular network providers, and governments to work to mitigate it. Moreover, the potential use of the Stingray in the commercial marketplace, whether as part of corporate espionage or furthering covert marketing efforts, makes the Stingray an important issue. Perhaps increasing use of the Stingray — and the associated opportunity for collection of information on innocent third parties — is an issue that is more likely to impact the general public than law enforcement's request for a court order to provide assistance in hacking into a defendant's cellphone for historical information.

---

[1] Most decisions appear to address law enforcement's acquisition of real-time cell phone location data from cellphone providers, rather than Stingray devices. The majority rule seems to be that a showing of probable cause is required in order to access such data, although courts in a minority of jurisdictions disagree. See United States v. Powell, 943 F. Supp. 2d 759, 770 – 73 (collecting cases), 778 – 79 (setting forth specific probable cause showings required for a warrant for "long-term real-time tracking of an individual via a cell phone") (E.D. Mich. 2013).

[2] This decision has been sealed by the court, see 2012 U.S. Dist. LEXIS 188033, but is available here.

[3] Rigmaiden, 2013 U.S. Dist. LEXIS 65633, at *60 – 64.

[4] In re United States, 2015 U.S. Dist. LEXIS 151811, at *14 – 15 (N.D. Ill., Nov. 9, 2015).

[5] https://www.justice.gov/opa/file/767321/download. The Department of Homeland Security's policy, dated October 19, 2015, is essentially the same as DOJ's in terms of its warrant requirements. See here.

[6] https://www.justice.gov/opa/file/767321/download. According to the Electronic Frontier Foundation, this warrant requirement only applies to criminal investigations. See here.

[7] https://www.justice.gov/opa/file/767321/download.

[8] https://www.justice.gov/opa/file/767321/download.

[9] https://www.justice.gov/opa/file/767321/download.

[10] https://www.justice.gov/opa/file/767321/download. DHS's guidance lists use of cell-site simulators "in furtherance of protective duties" of the Secret Service and the Secret Service Uniformed Division as an example of the sort of circumstance that would fall into this category. See here.

[11] Stephanie K. Pell and Christopher Soghoian, Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy, 28 Harv. J. Law & Tec 1, 46 (2014).

[12] Id.; see also here.

[13] http://www.wired.com/2010/07/intercepting-cell-phone-calls/.

[14] https://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html.

RELATED INDUSTRIES

- Technology

RELATED PRACTICES

- Litigation
- Privacy & Data Security
- Cybersecurity Incident Response
