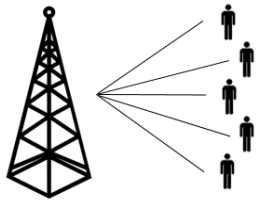
Cell Site Simulators

*A National Association of Criminal Defense Lawyers (NACDL) Primer**

WHAT IS A CELL SITE SIMULATOR?

A cell site simulator, frequently referred to as a Stingray or IMSI catcher, is a device that masquerades as a cell tower. It forces all cell phones in the vicinity that use the impersonated network to surreptitiously share information with it. Cell site simulators are portable, briefcase-sized devices, which can fit in small cars, be carried by hand, and even be deployed on airplanes to facilitate larger-scale surveillance.[1]

REGULAR CELL PHONE COMMUNICATIONS



COMMUNICATIONS WITH A CELL SITE SIMULATOR

HOW ARE CELL SITE SIMULATORS USED?

When a particular cell phone's unique identifiers[2] are known, a cell site simulator can locate and track the cell phone owner's movements.[3] When a suspect's cell phone's unique identifiers are unknown, such as when the suspect is using a "burner phone,"[4] a cell site simulator can acquire them.[5] Acquiring a cell phone's unique identifiers facilitates further surveillance, including wiretaps and the collection of call records.[6] Although some cell site simulators can also intercept the contents of communications,[7] most federal law enforcement agencies are subject to policies that prohibit the practice, and some local law enforcement agencies have said that their devices lack this capability.[8] Since cell site simulators collect identifying data from nearby bystanders' cell phones, they collect information relating to large numbers of people.

JUDICIAL AUTHORIZATION

Under recently issued policies, the U.S. Department of Justice and the U.S. Department of Homeland Security require their component agencies to obtain a search warrant supported by probable cause prior to using a cell site simulator, though neither department requires a warrant for "exigent" and "exceptional" circumstances.[9] In addition, through statutory and case law, the warrantless collection of cell phone location information is prohibited in some states, and the thresholds for obtaining a warrant vary.[10] Still, law enforcement agencies have used cell site simulators either without court authorization, or under court authorization obtained under the Pen Register Statute, which requires only a showing of relevance.[11] Pen register applications

---

[1] One type of cell site simulator deployed on airplanes is known as a "Dirtbox" or "DRT box." *See* Kim Zetter, *California Police Used Stingrays in Planes to Spy on Phones*, Wired (Jan. 27, 2016, 6:28 PM), http://www.wired.com/2016/01/california-police-used-stingrays-in-planes-to-spy-on-phones/.

[2] Basic numeric identifiers include the International Mobile Equipment Identity (IMEI), a unique number assigned to each handset, and the International Mobile Subscriber Identity (IMSI), a unique number assigned to each SIM card.

[3] The location of a cell phone can be captured within a range of a few meters. *See* Linda Lye, *Stingrays: The Most Common Surveillance Tool the Government Won't Tell You About*, ACLU of Northern California (2014), https://www.aclunc.org/sites/default/files/StingRays_The_Most_Common_Surveillance_Tool_the_Govt_Won't_Tell_You_About_0.pdf, at endnote 19.

[4] *Burner Phone*, Electronic Frontier Foundation, https://ssd.eff.org/en/glossary/burner-phone (last visited Apr. 16, 2016, 6:41 PM).

[5] U.S. Dep't of Homeland Security, Policy Directive 047-02 (Oct. 2015), https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf, at 2.

[6] Call detail records include the following information in relation to a phone call: time, duration, historical cell phone location information, completion status, source number, and destination number.

[7] "Contents" of a communication are defined in 18 U.S.C. § 2510(8). Contents cannot be intercepted without a Title III wiretap order issued under the provisions of 18 U.S.C. §§ 2510-2522, or an equivalent state law. For a list of states with statutes authorizing wiretaps and their accompanying citations, *see Wiretap Report 2014*, U.S. Courts (Dec. 2014), http://www.uscourts.gov/file/18177/download.

[8] The U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS) prohibit their component agencies' use of cell site simulators for capturing contents. U.S. Dep't of Justice, Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download, at 2; U.S. Dep't of Homeland Security, *supra* note 5, at 3. State and local law enforcement's use is governed by their own unique policies or no policies at all. *Infra* note 10 and accompanying text.

[9] Exigent circumstances include the need to protect human life, prevent the imminent destruction of evidence, pursue a fleeing felon, and prevent the escape of a suspect or convict. Exceptional circumstances are not listed, but include the need to carry out protective duties under 18 U.S.C. § 3056 and § 3056A (pertaining to the U.S. Secret Service). U.S. Dep't of Justice, *supra* note 8, at 3-5; U.S. Dep't of Homeland Security, *supra* note 5, at 4-5. Before the new policies were issued, the DOJ and DHS generally advised in favor of obtaining either an order under the Pen Register Statute, 18 U.S.C. § 3123, alone, or a 'hybrid' order under the combined authority of the Pen Register Statute and the Stored Communications Act, 18 U.S.C. § 2703(d).

[10] As of October 2015, these states include California, Colorado, Florida, Illinois, Indiana, Maine, Maryland, Minnesota, Montana, New Hampshire, New Jersey, Tennessee, Utah, Virginia, Washington, and Wisconsin. The warrant requirements vary according to the type of cell phone location information being sought. Peter Cihon, *Status of Location Privacy Legislation in the States: 2015*, ACLU Blog (Aug. 26, 2015, 1:15 PM, updated Oct. 13, 2015), https://www.aclu.org/blog/free-future/status-location-privacy-legislation-states-2015.

[11] The Federal Bureau of Investigation (FBI) has required many state and local law enforcement agencies to sign non-disclosure agreements prohibiting disclosure in any civil or criminal proceeding of information concerning cell site simulators without its prior written approval. *See, e.g.*, *Andrews*, *infra* note 16, at 22-25. *See also Non-Disclosure Agreements Between FBI and Local Law Enforcement for StingRay*, The Center for Human Rights and Privacy,

* This primer was prepared in partnership with the Samuelson Law, Technology & Public Policy Clinic at UC Berkeley, School of Law with the assistance of Bhairav Acharya, Richa Goyal, and Jaideep Reddy.

have often misled courts by describing the device merely as a pen register or "confidential source," thereby concealing its true surveillance capacity.[12] Particularly for agencies not subject to state legislation or new policies, these practices may be ongoing.

HOW TO DETECT ITS USAGE IN YOUR CASE

Cell site simulators appear to be in widespread use; however, it is not always easy to recognize when one was used. There are several indicators to watch for that may suggest cell site simulator use in your client's case:

1. Terminology: The government may use a range of terms to refer to a cell site simulator, including: digital analyzer, cell site emulator, cell site monitor, IMSI catcher, and WITT. The government may also refer to the device by a trade name, including Stingray, Triggerfish, Kingfish, Amberjack, and Hailstorm. However, because there is a high level of secrecy surrounding these devices, the government may instead use broad and/or imprecise terms such as "mobile tracking device" or "pen register," which gloss over the technical capabilities of a cell site simulator.
2. Source Explanations: Law enforcement may have used a cell site simulator when government evidence contains highly precise information about a person's location or reveals knowledge of a cell phone's unique numeric identifier that is unsupported by a credible source explanation. This includes information that cites a "confidential source" or "known investigative technique" without an adequate explanation. Information attributed to a confidential informant with a minimal or non-existent criminal record bears deeper scrutiny.

POTENTIAL LEGAL ARGUMENTS

1. Discovery: If you have reason to believe that a cell site simulator was used against your client, such as an unconvincing explanation for how your client was located, consider making detailed requests in discovery[13] about whether the device was used,[14] and if so, how. If insufficient information is provided at first, consider a motion to compel.
2. Exclusion: Consider the following arguments to exclude evidence collected by a cell site simulator in your case:
    a. *Fourth Amendment Suppression*:[15]
        i. The use of a cell site simulator implicates the Fourth Amendment and needs to be supported by a warrant based on probable cause.[16] Statutory orders such as a pen/trap or hybrid orders that are issued on a standard lower than probable cause do not suffice because cell site simulators are much more invasive than pen registers.[17]
        ii. Even a warrant authorizing the use of cell site simulators should be presumed invalid because the use amounts to a "general search," violating the Fourth Amendment's particularity requirement.[18]
        iii. The government's application for judicial authorization contained material omissions.[19]
    b. *Admissibility*: A *Daubert*/*Frye*[20] hearing is required to ascertain the qualifications of expert witnesses and the reliability of their testimony on the use of the cell site simulator.

SELECTED RESOURCES

1. C. Justin Brown and Kasha M. Leese, *StingRay Devices Usher in a New Fourth Amendment Battleground*, The Champion (2015), http://www.nacdl.org/Champion.aspx?id=37742&terms=stingray.
2. *State v. Andrews*, No. 1496 (Md. Ct. Spec. App. 2016), http://www.mdcourts.gov/opinions/cosa/2016/1496s15.pdf (a well-reasoned opinion granting suppression of cell site simulator evidence, the first case in which this has been done).
3. Linda Lye, *Stingrays: The Most Common Surveillance Tool the Government Won't Tell You About*, ACLU (2014), https://www.aclunc.org/sites/default/files/StingRays_The_Most_Common_Surveillance_Tool_the_Govt_Won't_Tell_You_About_0.pdf (describing the technology, government use, legal authority, and suggested legal arguments).
4. Br. of the American Civil Liberties Union et al. as Amici Curiae, *Prince Jones v. United States* (D.C. 2016), https://www.aclu.org/legal-document/prince-jones-v-united-states-amicus-brief (articulating the Fourth Amendment arguments against the use of cell site simulators).

---

http://www.cehrp.org/non-disclosure-agreements-between-fbi-and-local-law-enforcement/ (last visited Apr. 16, 2014).

[12] Lye, *supra* note 3 at 1, 4.

[13] *See id.* at 23-26 (providing a sample discovery list relating to cell site simulators).

[14] Avoid reference to trade names, like Stingray, since law enforcement could avoid providing information if they did not use that particular device.

[15] In March 2016, the Maryland Court of Special Appeals allowed suppression of cell site simulator evidence on Fourth Amendment grounds, in the first case in which this has been done. *State v. Andrews*, No. 1496 (Md. Ct. Spec. App. 2016), http://www.mdcourts.gov/opinions/cosa/2016/1496s15.pdf, at 65-69.

[16] *Andrews*, No. 1496, at 25-44; Br. of the Electronic Frontier Foundation et. al. as Amici Curiae at 18-24, *United States v. Patrick* (7th Cir. Mar. 9, 2016), https://www.eff.org/document/us-v-patrick-eff-amicus; Br. of the American Civil Liberties Union et al. as Amici Curiae at 2-10, *Jones v. United States* (D.C. Cir. Nov. 3, 2015), https://www.aclu.org/legal-document/prince-jones-v-united-states-amicus-brief.

[17] *See* Lye, *supra* note 3 at 14-15.

[18] *See id.* at 13-14; Br. of the American Civil Liberties Union et al. as Amici Curiae at 9-10, *State v. Andrews* (Md. Ct. Spec. App. 2015), https://www.eff.org/document/state-maryland-v-andrews-effaclu-amicus-brief-stingrays.

[19] Lye, *supra* note 3 at 16-19. This argument can also be used to request a *Franks* hearing as an alternative to suppression. *Franks v. Delaware*, 438 U.S. 154 (1978); *see also* Br. of the American Civil Liberties Union et al. as Amici Curiae, *supra* note 18, at 10-15.

[20] *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993); *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923).