UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
WESTERN DIVISION

In the Matter of the Application of the United States of America for an Order Relating to Telephones Used by Suppressed	) No. 15 M 0021) Iain D. Johnston) U.S. Magistrate Judge

MEMORANDUM OPINION AND ORDER

This opinion explains this Court's requirements relating to the use of cell-site simulators in a typical drug-trafficking investigation. To date, the requirements outlined in this opinion have not interfered with effective law enforcement.

I. Facts

A. Investigatory Facts

The basic facts relating to the investigation are unsurprising. A target of an investigation is allegedly distributing, through a conspiracy, a large amount of controlled substances in the Northern District of Illinois, in violation of 21 U.S.C. §§ 841(a), 846. The target frequently uses a cell phone as part of the conspiracy to distribute the controlled substances. This target frequently discards the cell phone after a period of time and obtains a new cell phone to continue to distribute the controlled substances. This target obtains cell phones by using fictitious identifying information. During the investigation, this target discarded the cell phone that had previously been used, and obtained a new cell phone. The United States of America seeks to obtain the new telephone number for the new cell phone to continue its investigation.

Although the investigative facts are unsurprising, the method and technology used to obtain the cell phone number may be surprising to many people. The United States has submitted an application for a warrant to use a cell-site simulator to obtain this target's new cell phone number.

B. What is a Cell-Site Simulator?

Unfortunately, the manufacturer of cell-site simulators (a company called the Harris Corporation) is extremely protective about information regarding its device. In fact, Harris is so protective that it has been widely reported that prosecutors are negotiating plea deals far below what they could obtain so as to not disclose cell-site simulator information. Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, Washington Post, February 22, 2015. Indeed, Harris requires law enforcement officers, and others, to sign non-disclosure agreements (NDAs) regarding the devices. Ernest Reith Acting Assistant Director of the Fed. Bureau of Investigation, Baltimore Police Department Non-Disclosure Agreement (July 13, 2011), http://s3.documentcloud.org/documents/1808819/baltimore-police-stingray-non-disclosure-agreement.pdf.

So where is one, including a federal judge, able to learn about cell-site simulators? A judge can ask a requesting Assistant United States Attorney or a federal agent, but they are tight lipped about the device, too; in all likelihood because of the NDAs. Jack Gillum, *Feds Urge Quiet on Spying Technology*, The Spokesman-Review (June 13, 2014),

http://www.spokesman.com/stories/2014/jun/13/feds-urge-quiet-on-spying-techology/. The Court could attempt to learn about the device on the Internet. *See* Stingray Phone Tracker, http://en.wikipedia.org/wiki/Stingray_phone_tracker (last visited October 19, 2015). But most reasonable people know to be highly skeptical about what they read on the Internet, particularly in Wikipedia posts. *United States v. Lawson*, 677 F.3d 629, 650-51 (4th Cir. 2012) (collecting federal decisions expressing concern regarding Wikipedia's reliability); *Crispin v. Audigier, Inc.*, 717 F. Supp. 2d 965, 976 n.19 (C.D. Cal. 2010) (collecting authority noting danger of relying on Wikipedia).[1] Cell-site simulators are also the topic of many recent law review articles. *See, e.g.*, Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Technology*, 16 Yale J.L. & Tech. 134 (2013-2014). A good overview of cell-site simulators was recently discussed in *The Champion*. C. Justin Brown & Kasha M. Leese, *StingRay Devices Usher in a New Fourth Amendment Battleground*, The

[1] Indeed, the concern of Wikipedia entry accuracy is recognized in popular culture. *See, e.g.,* The Big Bang Theory, *The Pirate Solution* (Series 3, Episode 4) (when asked by Leonard what he was doing for six months, Raj explains that he was busy checking e-mail, updating his Facebook status and "messing up Wikipedia entries"); 30 Rock, *Cleveland*, (Season 1, Episode 20) ("Ah, well, it must be true if it's on the 'Interweb.'") Additionally, the Court is aware of Judge Hamilton's well-reasoned and well-stated concerns in *Rowe v. Gibson*, 798 F.3d 622, 638-44 (7h Cir. 2015) (Hamilton, J., dissenting in part) regarding judicial internet research, including the reliability of internet research.

The requirements in this opinion establishing the use of a cell-site simulator do not violate those concerns for several reasons. First, the application process is *ex parte*. Second, before imposing the requirements, the Court gave the United States government the opportunity to explain the use and technology of cell-site simulators, as well as, importantly, the opportunity to express concerns about the requirements based upon the Court's understanding of the use and technology. Third, the matter is in the investigative stage, not the merits stage.

Champion, June 2015, at 12. But those articles often rely on secondary source material, including the possibly untrustworthy Internet websites. Unfortunately, the one place where a person will be unable to find much discussion of cell-site simulators is case law. *In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012) ("Regardless of what it is called, there is scant case law addressing the equipment."). And even case law that discusses stingrays refers to newspaper reports as authority on these devices. *See, e.g., Wisconsin v. Tate*, 849 N.W.2d 798, 802 n.8 (2014) (citing Jenifer Valentio-DeVries, *"Stingray" Phone Tracker Fuels Constitutional Clash*, Wall Street Journal, September 22, 2011).

Despite all the confidentiality surrounding cell-site simulators, an excellent source of information regarding the device is published by the Department of Justice. *See* Department of Justice, Electronic Surveillance Manual (June 2005), http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. When presented with an application to use a cell-site simulator, at a minimum, courts should review this document to understand exactly what the United States is requesting of the court. Some commentators argue that judges may be allowing the use of cell-site simulators without possessing a complete understanding of the device and how it works, because, in part, the information is buried in technical jargon in the application. Pell & Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap*, 16 Yale J.L. & Tech. at 160; Brown & Leese, *StingRay Devices Usher in a*

New Fourth Amendment Battleground, The Champion, at 16. This Court does not know whether that argument is accurate, in part, because of the dearth of case law discussing these devices.[2]

The Court has spent a considerable amount of time collecting information relating to cell-site simulators. The following is the Court's understanding of the device. A cell-site simulator goes by many different names, including, but not limited to "stingray," "triggerfish" and "kingfish."[3] Although these devices were also previously called "digital analyzers," the moniker "cell-site simulator" is the most self-explanatory. The device does exactly what the name describes: it simulates a cell site. And by simulating a cell site, the device causes or forces cell-phones in an area to send their signals – with all the information contained therein – to the cell-site simulator. Once the cell phones in the area send their signals to the cell-site simulator, the device captures a vast array of information, including, but not limited to, the cell phones' electronic serial number ("ESN") or international mobile subscriber identification ("IMSI"). A cell phone need only be on for the cell-site simulator to capture the cell phone's ESN and IMSI; the cell phone need not be "in

[2] The undersigned was a friend of the late Kurt F. Schmid, the former Chicago HIDTA Director. Kurt was a fantastic law enforcement officer and phenomenal person. Kurt provided non-confidential information to the undersigned to attempt to corroborate the information the undersigned collected. Kurt Schmid's recent passing is a loss to those who strived for effective and constitutional law enforcement. The undersigned is grateful to Kurt Schmid for his friendship and help in understanding cell-site simulators, among many other things.

[3] Apparently, having exhausted the ichthyological theme, law enforcement has started referring to cell-site simulators as "superdog." Hopefully, this new moniker is an homage to the famous drive-in restaurant, located at the intersection of Milwaukee, Devon and Nagle, and operated by the great Berman family. *See* Superdawg Drive-In, http://www.superdawg.com (last visited Oct. 19, 2015).

use."[4] The cell-site simulators signals penetrate structures, just as cell phones' signals penetrate most structures. Although the operator of a cell-site simulator can use a directional antenna to direct the simulator's signal toward a certain area (sometimes referred to as "directional finding"), the cell-site simulator will still force many innocent third parties' cell phones to direct their signals to the simulator.

Armed with a cell-site simulator, a law enforcement officer can obtain a target's cell phone's ESN or IMSI (among many other things) by taking the device near the physical location of the target's cell phone and then activating the device. By activating the device, the cell phones in a geographical area will send their signals to the device, which in turn captures the information. This process can be repeated at a later time and different location so that the target's cell phone ESN or IMSI can be identified among all the other cell phone telephone information previously captured. (Basically, by process of elimination, the target's cell phone number is identified.) According to the application submitted to the Court, with the ESN or IMSI, the United States can subpoena the service provider to obtain the cell phone's telephone number. However, according to the Department of Justice, a cell site simulator can collect a cell phone's telephone number directly; thereby eliminating this step.

Now possessing the target's cell phone telephone number, the United States can return to a judicial officer with an application for a trap and trace and/or pen

[4] Today, cell phones are essentially always on. At any given moment, even when the owner is not speaking on the cell phone, the cell phone can be receiving emails, text messages, and location information about their children's cell phones, among other things. Even while being charged, cell phones are on.

registry to obtain information regarding the use of the phone or even obtain a wire-tap for that phone from a District Court Judge. *See* 18 U.S.C. § 2518 (wiretap); 18 U.S.C. § 3123 (pen registry and trap and trace).

II. Constitutional Concerns

The use of cell-site simulators raises numerous Fourth Amendment concerns. The main concern is whether the use of a cell-site simulator implicates the Fourth Amendment's probable cause requirement. *In re the Application of the U.S. for an Order*, 890 F. Supp. 2d at 752; *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 996 n.6 (D. Ariz. 2012) (government conceded that the Fourth Amendment's probable cause standard applied). Luckily for the Court, the application in this case recognizes the need to meet the probable cause standard, and, in fact, easily meets that standard. Indeed, recently, the United States Department of Justice has required federal agents to meet the probable cause standard in most circumstances. Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015), http://www.justice.gov/opa/file/767321/download.

Because there is no dispute that a warrant meeting the probable cause standard is necessary to use a cell-site simulator under these circumstances, the Court addresses a different but similarly important issue. This opinion focuses on the collection of innocent third parties' information, an occurrence that appears inevitable by the cell-site simulator's use. As shown below, the Court believes that a process must be created to reasonably ensure that innocent third parties' information collected by the use of a cell-site simulator is not retained by the United

States or any government body. The concern over the collection of innocent third parties' information is not theoretical. It has been reported that the federal government collects telephone numbers, maintains those numbers in a database and then is very reluctant to disclose this information. *See* Defendant's Motion to Suppress Evidence at 17-19, *United States v. Hassanshahi*, No. 1:13-cr-00274-RC (D.D.C. Mar. 27, 2014), ECF No. 28; Zoe Tillman, *Judge Questions Feds' "Mysterious" Phone Database*, National Law Journal, Dec. 8, 2014, at 19. Moreover, even in the civil litigation context, third parties have more privacy interests and are afforded more court protections than litigants. *McGreal v. AT&T Corp.*, 892 F. Supp. 2d 996, 1010 (N.D. Ill. 2012).

III. Requirements for the Use of a Cell-Site Simulator

When a cell-site simulator is used, the Court will impose three requirements: the first relates to the manner in which the device is used; the second relates to the destruction of innocent third parties' data; and the third explicitly prohibits the use of innocent third parties' data. *See generally* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. Pa. J. Const. L. 1, 45-47 (2013).

First, law enforcement officers must make reasonable efforts to minimize the capture of signals emitted from cell phones used by people other than the target of the investigation. For example, when appropriate, law enforcement officers must use methods available to direct the cell-site simulator's signal. Moreover, law enforcement officers must not use a cell-site simulator when, because of the location

and time, an inordinate number of innocent third parties' information will be collected. A hyperbolic example of this requirement would prohibit law enforcement officers from using the device outside the BMO Harris Bank Center during a Rockford Ice Hogs[5] game or a high school graduation.[6] Reasonable law enforcement officers would have no quarrel with this requirement. Indeed, their own self-interest is served in minimizing the amount of innocent third parties' cell phone information that is collected. The additional information only complicates the process of identifying the target's cell phone ESN or ISMI.

Second, law enforcement officers must immediately destroy all data other than the data identifying the cell phone used by the target. The destruction must occur within forty-eight hours after the data is captured. The forty-eight hour time frame is designed to have some consistency with other Fourth Amendment principles, such as promptly presenting a defendant before a neutral and detached magistrate judge for a probable cause determination, seeking a warrant for an overhear device when one cannot be obtained beforehand because of an emergency, and obtaining, after the fact, an order for a pen registry and trap and trace when one could not be previously obtained because of an emergency. *See County of Riverside v. McLaughlin*, 500 U.S. 44 (1991); 18 U.S.C. § 2518(7); 18 U.S.C. § 3125(a)(2). Additionally, the destruction must be evidenced by a verification provided to the Court with the return of the warrant. In civil litigation, protective

[5] The Rockford Ice Hogs are the proud American Hockey League affiliate of the mighty Chicago Blackhawks of the National Hockey League. The Ice Hogs play their home games at the BMO Harris Bank Center.

[6] Each spring, many Rockford high schools hold their graduations in the BMO Harris Bank Center.

orders and confidentiality orders often contain provisions requiring a party to certify that confidential documents have been destroyed at the termination of the case. Indeed, the U.S. District Court for the Northern District of Illinois' own model confidentiality order form contains a similar provision. Model Confidentiality Order Pursuant to Local Rule 26.2, United States District Court Northern District of Illinois, at 10 (June 29, 2012), http://www.ilnd.uscourts.gov/_assets/_documents/OnlineForms/26.2%20FORM.pdf. Furthermore, because the United States will be returning the warrant at a later date, the additional requirement mandating that the verification be returned at the same time is minimal at most.

Third, law enforcement officers are prohibited from using any data acquired beyond that necessary to determine the cell phone information of the target. A cell-site simulator is simply too powerful of a device to be used and the information captured by it too vast to allow its use without specific authorization from a fully informed court. Minimizing procedures such as the destruction of private information the United States has no right to keep are necessary to protect the goals of the Fourth Amendment. *See In the Matter of the Search of Information Associated with the Facebook Account Identified by the Username AA Ron.Alexis That is Stored at Premises Controlled by Facebook Inc.*, 21 F. Supp. 3d 1, 9-10 (D.D.C. 2013).

Accordingly, this Court requires that the order granting the application must contain a provision that reads as follows: "The Federal Bureau of Investigation, and

other authorized law enforcement officials, may employ electronic investigative techniques to capture and analyze signals emitted by any and all cellular telephones used by [the target] for a period of 30 days. Officials of the Federal Bureau of Investigation and other authorized law enforcement officials (a) must make reasonable efforts to minimize the capture of signals emitted from cellular telephones used by people other than [the target], (b) must immediately destroy all data other than the data identifying the cellular telephones used by [the target] (such destruction must occur within forty-eight (48) hours after the data is captured, and the destruction must be evidenced by a verification provided to the Court with the return of the warrant), and (c) are prohibited from using the data acquired beyond that necessary to determine the cellular telephones used by [the target]."

* * *

The minimizing procedures outlined in this opinion and required by this Order are designed to reasonably balance the competing interests of effective law enforcement and people's Fourth Amendment privacy interests.

Entered: November 9, 2015 By: _____

Iain D. Johnston
U.S. Magistrate Judge