IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	
v.	*	**Criminal No. CCB-14-170**
ROBERT HARRISON	*	

* * * * * * * * * * * * *

MOTION TO SUPPRESS EVIDENCE
RESULTING FROM USE OF CELL SITE SIMULATOR

Robert Harrison, through his undersigned counsel, C. Justin Brown, hereby moves this Honorable Court to suppress evidence obtained as a result of the Government's unconstitutional search of Harrison and his residence at 3805 Chatham Road in Baltimore, Maryland, by means of a cell site simulator, a/k/a "Stingray," device. The Government's use of a cell site simulator constitutes a warrantless search of Harrison's apartment, person, and phone, in violation of the Fourth Amendment. Each of these unconstitutional searches is an independent ground for suppression.

I. BACKGROUND

A. Factual Background of This Case

Harrison is charged with Conspiracy to Use Interstate Commerce Facilities in the Commission of Murder-For-Hire, in violation of Title 18 U.S.C. § 1958.

The Government's theory is that Harrison was enlisted by co-defendant Derrick Smith to assist with a fictitious murder-for-hire plot. According to discovery provided by the Government, the plot originated with information provided to law enforcement by a confidential source ("CW1"). CW1 told authorities that Smith was a hit man for hire and, under the supervision of

law enforcement, CW1 initiated contact with Smith to propose that Smith commit a fictitious murder.

CW1 worked with an undercover police officer ("UC") to convince Smith to agree to the plot. On February 4, 2014, the UC provided Smith with a cellular telephone, telephone number ending in the number "6749" (the "phone"). In the weeks leading up to Smith's arrest, CW1 and UC placed multiple phone calls to the phone. Some of the calls were answered by individuals other than Smith. The Government theorizes that one of the people who used the phone was Harrison.

On February 5, 2014, the Circuit Court of Baltimore City entered an Order authorizing the use of a device, known as a "Pen Register \ Trap & Trace and Cellular Tracking Device to include cell site information, call, detail, without geographical limits" on the phone. (Ex. 1). The Order was based on an Application[1] by Baltimore Police Department Detective Julie Pitocchelli, pursuant to Section 10-4B-04 of the Courts and Judicial Proceedings Article of the Maryland Code ("Section 10-4B-04"). *See* Ex. 1. Neither the Application nor the Order contained an ascertainable description of the cell site simulator/Stingray. *See* Ex. 1.

As some time prior to the arrest of Smith, the Government turned its attention to the phone, and attempted to figure out who was using it, and where they were using it. According to the AUSA handling the case, the Stingray device[2] was then employed to pinpoint where the

[1] The Application also contained what is arguably a misrepresentation of material fact, to wit, that "Derrick Smith . . . has been contracted to kill another unknown male." Ex. 1 at ¶ 1. In reality, the "unknown male" was not a real person—he was fictitious. Use of the words "unknown male," created an appearance of imminent harm when no such threat existed.

[2] The Government has not specifically called the device a "Stingray," however the brief description of its use, as provided by the case agent and the prosecutor, is consistent with how a "Stingray" is used. For the sake of convenience, this Motion will refer to it as a "Stingray" or, more generally, a "cell site simulator."

phone was located. Through use of Stingray technology, Baltimore City police learned that the phone was located at, precisely, 3805 Chatham Road.

Once police learned of this address, according to an FBI 302 report,[3] police used open-source databases to obtain the names of the residents living at 3805 Chatham Road. The agents then cross-referenced those names with information related to Derrick Smith, according to the report, and found multiple connections between Smith and Harrison. Based on this, Harrison was suspected to be an accomplice of Smith.

On March 27, 2014, a team of approximately five Baltimore City police officers and detectives approached Harrison's apartment, where he lived with his girlfriend and several children. The officers now claim that Harrison consented to their entry and search of his apartment. Harrison maintains that he did not consent and they made a forced entry.

Once inside the apartment, police conducted a search and found the cellular phone they had been tracking with the Stingray device. At some point after the arrest, upon speaking to Harrison, officers were able to match Harrison's voice to one of the voices on a controlled call previously made by CW1. The Government asserts that Harrison made an incriminating statement during that call, which is the basis for the federal criminal charges.

B. Technical Background of Cell Site Simulators

Ordinarily, wireless carriers provide coverage through a network of base stations, also called "cell sites," which connect wireless devices to the carrier's network. Cell phones periodically identify themselves to the base station that has the strongest radio signal, which is

[3] The report was prepared by FBI Agent Eric Nye on September 3, 2014 – six months after the date of the arrest – in response to a request by undersigned counsel for more information about the incident.

often, but not always, the nearest base station.[4] A cell phone automatically transmits to the base station "signaling data," which includes the phone's unique numeric identifier, as well as its cell site code, which identifies its location.[5]

A cell site simulator, also known as a Stingray,[6] IMSI[7] catcher, triggerfish, or digital analyzer,[8] is a technology that can triangulate the source of a cellular signal without going through the wireless carrier. Instead, the technology mimics a carrier's cell phone towers and measures the strength of the cellular signal from several locations. Essentially, it masquerades as a wireless carrier's base station and electronically forces a cell phone to communicate with it as if it were the carrier's base station.[9] By using cell site simulators, the Government can locate, interfere with, and intercept communications from cell phones and other wireless devices.[10]

---

[4] *See* Testimony of Matt Blaze during Hearing on EPCA Reform and the Revolution in Location Based Technologies and Services before the House Cmte. on the Judiciary, Subcmte. on the Constitution, Civil Rights and Civil Liberties, at 4 (June 24, 2010), *available at* http://crypto.com/papers/blaze-judiciary-20100624.pdf.

[5] *See* DOJ Electronic Surveillance Manual (Jan. 2, 2008), *included in* DOJ's Response to ACLU's FOIA Request at 17 (Aug. 12, 2008), *available at* https://www.aclu.org/files/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (hereinafter cited as "DOJ Electronic Surveillance Manual," and citations will refer to the pagination of the FOIA Request Response PDF).

[6] "Stingray" is the name for a cell site simulator sold by the Harris Corporation.

[7] IMSI is the acronym for "international mobile subscriber identity," which is a cell phone's unique identifier.

[8] *See* DOJ Electronic Surveillance Manual at 17.

[9] *See id.* at 41 ("A cell site simulator (CSS) electronically "forces" a cellular telephone to autonomously register its MIN and ESN when the target telephone is turned on but is not being used.").

[10] *See* ELECTRONIC PRIVACY INFORMATION CENTER ("EPIC"), *Epic v. FBI – Stringray / Cell site simulator*, http://epic.org/foia/fbi/stingray/.

The Department of Justice Electronic Surveillance Manual describes the capabilities of cell site simulators:

> The equipment includes an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information. Working together, these devices allow the agent to identify the direction (on a 360 degree display) and signal strength of a particular cell phone while the user is making a call. By shifting the location of the device, the operator can determine the phone's location more precisely using triangulation.[11]

The Manual also explains the various benefits to law enforcement agencies of using cell site simulators:

> If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/triggerfish [a.k.a. cell site simulator] would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected). . . . [Cell site simulators] and similar devices may be capable of intercepting the contents of communications[.][12]

Law enforcement agencies can also use cell site simulators to determine a phone's location if they know the target cell phone's IMSI. The IMSI is programmed into the cell site simulator, which then sorts through the signaling data (including location) of cell phones in the area until it finds a match. Simultaneously, law enforcement agencies may also obtain information through requests to carriers for cell site location information. Cell site simulators vary from carrier requests in at least two important ways.

First, cell site simulators can typically be used without carrier assistance. With carrier-assisted surveillance, the carrier necessarily has knowledge that the surveillance is taking place and has copies of the records it discloses at the request of law enforcement pursuant to a

[11] DOJ Electronic Surveillance Manual at 9.

[12] *Id.* at 17.

traditional pen register/trap and trace order. By bypassing the carrier and using a cell site simulator, only the operator of the device has knowledge that an interception ever took place and has access to the intercepted information (as is the case here). To the extent that carriers may be able to act as a proxy for their customers' privacy interests and push back against some law enforcement requests, no such advocates exist when a cell site simulator is used.

Second, cell site simulators produce extremely precise location information, in some cases within an accuracy of two meters (approximately six feet).[13] In one federal case, the Government conceded that the cell site simulator located the defendant's wireless device precisely within a specific apartment in an apartment complex.[14] In Florida, Tallahassee police testified that by "using portable equipment" and going to "every door and window" in a large apartment complex, they were able to identify the "particular area of the apartment that the handset was emanating from."[15]

Additionally, cell site simulators differ from carrier requests because they are capable of capturing the content of communications, such as voice calls and text messages.[16] They also obtain information from third parties, not just the target phone. Finally, they force the target phone to emit a signal. The aforementioned differences capture the distinct nature and

---

[13] *See, e.g.,* PKI Electronic Intelligence, GSM Cellular Monitoring System (product brochure) at 12, http:// docstoc.com/docs/99662489/GSM-CELLULAR-MONITORING-SYSTEM (noting that the device can "locat[e] . . . a target mobile phone with an accuracy of 2 m[eters]").

[14] *See United States v. Rigmaiden*, 844 F. Supp. 2d 982, 996 (D. Ariz. 2012).

[15] Hearing on Motion to Suppress, *Florida v. Thomas*, No. 2008-CF-3350A (Fla., Leon Co. Cir. Ct., Aug. 23, 2010), *available at* https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf.

[16] *See* DOJ Electronic Surveillance Manual at 17. The devices used by the federal Government are likely configured to disable the content-interception function, as the DOJ has acknowledged that a wiretap order under the heightened Title III standard (18 U.S.C. § 2518) would otherwise be necessary. *See id.*

intrusiveness of the Government's use of cell site simulators, but they are only some of the facts obtained through various organizations' FOIA requests; there may be more.

II. LEGAL ARGUMENT

A. The Use of the Cell Site Simulator Violated the Fourth Amendment.

Law enforcement's use of the cell site simulator in this case constitutes a search of Harrison's apartment, phone, and person. Because that search was without a warrant and no exception to the warrant requirement applies, it was in violation of the Fourth Amendment.

1. Legal Standard

The Fourth Amendment is a fundamental bedrock of our criminal justice system to protect against the evils of "general warrants" and to safeguard our civil rights. *Payton v. New York*, 445 U.S. 573, 583 (1980). It provides the following:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

Warrantless searches are unreasonable unless one of several well-delineated exceptions to the warrant requirement applies. Further, "[i]t is a basic principle of Fourth Amendment law that searches and seizures inside a home are presumptively unreasonable." *Payton*, 445 U.S. at 586.

Here, law enforcement conducted a search of Harrison's apartment (his house), his phone (his effect), and his person (via the search of his phone). There was no warrant, and none of the exceptions apply. Therefore, the search was unreasonable, and it violated the Fourth Amendment.

2. There was no warrant.

The Government did not obtain a warrant for the use of the cell site simulator or other similar GPS monitoring/ surveillance tools that it used to locate Harrison. It did, however, submit an Application for the use of a Pen Register / Trap and Trace Device (the "Application") pursuant to Section 10-4B-04 of the Courts and Judicial Proceedings Article of the Maryland Code ("Section 10-4B-04"), and the Circuit Court entered an Order on February 5, 2014 (the "Order"). *See* Ex. 1. Undersigned counsel is unaware of whether the Government intends to argue that the Order covers its use of the cell site simulator. However, the Order does not mention the cell site simulator, is not a warrant, and does not obviate the need for a warrant.

In the Application, the Government stated it was seeking an "Order authorizing the installation and use of a device known as a Pen Register \ Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits, which registers telephone numbers dialed or pulsed or from or to" [the phone] pursuant to Section 10-4B-04. *See* Ex. 1 at 1. It went on to request that the Order include the following:

> Directing that the Agencies are authorized to employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of a Pen Register \ Trap & Trace and Cellular Tracking Device, unobtrusively and with a minimum of interference to the service of subscriber(s) of the aforesaid telephone, *and shall initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonably available, Global Position System Tracing and Tracking, Mobile Locator tools, R.T.T. (Real Time Tracking Tool), Precision Locations and any and all locations,* and such provider shall initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonable available and at such intervals and times as directed by the law enforcement agent / agencies serving the Order.

Ex. 1 at ¶ E (emphasis added).

The Application did not contain a definition or description of the terms emphasized above. The statutory authority for the Application and Order, Maryland Courts and Judicial

Proceedings Article of the Code of Maryland, Title 10, Subtitle 4B, also does not define these terms. Instead, Section 10-4B-04 authorizes only pen registers and trap and trace devices.[17]

The Application similarly lacks any reference to or description of a cell site simulator (which is also, unsurprisingly, omitted from Section 10-4B-04). No judge, however technologically savvy she may be, could understand from reading the aforementioned excerpt that the Government was seeking authority to use a cell site simulator..

There is scant case law on the Stingray device or other advanced cellular tracking tools. However, in *In re the Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 747, 752 (S.D. Tex. 2012), the court held that the Government's use of the Stingray device required a warrant, rather than a pen register order. It explained that the application for a pen register order had "a number of shortcomings[,]" such as the Government's failure to explain the technology, how the technology will be used, how may distinct surveillance sites on which it will operate the technology, or how long it intends to operate the technology. *See id.* at 749.

A case discussed there, *United States v. Rigmaiden*, 844 F. Supp 2d 982 (D. Ariz. 2012), also sheds light on the distinct differences between cell site simulators and pen registers and trap and trace devices. In *Rigmaiden*, the Government located the defendant based, in part, by tracking the location of an aircard connected to a laptop. For its investigation, the Government had both a pen register and a trap and trace device, as well as a warrant for a mobile tracking device. That court explained that the mobile tracking device used to locate the aircard functioned as a cell site simulator because it mimicked a cellular service provider's towers "and sent signals to, and received signals from, the aircard." *Id.* at 995. It observed that the mobile tracking device

[17] Title 10, Subpart 4B explicitly defines "pen register" and "trap and trace device" in Sections 10-4B-01, (c)(1) and (d)(1).

was "physically separate from the pen register trap and trace device used to collect information from" [the cellular service provider]. *Id.* The Government also asserted that, for the purposes of the motion to suppress in that case, the Court may assume that the tracking operation was a Fourth Amendment search and seizure. *Id.*

3. There was a search.

The Government's use of a cell site simulator was a search of Harrison's apartment, of the phone, and of Harrison's person (via the phone), all of which independently violated Harrison's Fourth Amendment rights.

a. The search of Harrison's apartment

The Government's use of the cell site simulator to learn about the contents of Harrison's apartment constituted a search. The cell site simulator was used to find out where the phone was, *i.e.*, whether it was in Harrison's apartment. Harrison's apartment is not a public place or thoroughfare—it is a private residence, a place where "the right to be free from warrantless governmental intrusion is unquestioned." *United States v. Karo*, 468 U.S. 705 (1984) (quoting *United States v. Karo*, 710 U.S. 1433 (10th Cir. 1984)).

The Supreme Court addressed electronic monitoring inside of a home in *United States v. Karo* and found that it was unconstitutional without a warrant. There, Government agents installed a beeper in a container of ether that was delivered to the defendant. They then used the beeper monitor to determine that the ether was in the defendant's residence, and they used this information to obtain a warrant to search the residence. *See id.* at 707–10. The court explained that, while the agents' monitoring of the beeper was less intrusive than a full-scale search of the home, it did "reveal a critical fact about the interior of the premises that the Government is

extremely interested in knowing and that it could not have obtained without a warrant[:]" that the ether was actually located in the defendant's house. *Id.* at 716; *see also id.* at 719.

Further, in deciding that the Government was required to obtain a warrant to monitor the beeper, the Court rejected several arguments by the Government:

> [We] reject the Government's contention that it would be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime . . . will be committed[.] . . . If agents are required to obtain warrants prior to monitoring a beeper when it has been withdrawn from public view, the Government argues, for all practical purposes they will be forced to obtain warrants in every case in which they seek to use a beeper, because they have no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises. The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.

Id. at 717–18.

Just like in *Karo*, here, the Government's use of the cell site simulator to obtain information about the presence of items in the interior of Harrison's apartment "reveal[ed] a critical fact" that the Government was interested in knowing and could not otherwise know without first obtaining a warrant to search the apartment. *Id.* at 716. It constitutes "[i]ndiscriminate monitoring of property that has been withdrawn from public view . . . [and, therefore,] present[s] far too serious a threat to privacy interests in the home to escape some sort of Fourth Amendment oversight[,]" *i.e.*, the warrant requirement.

b. The search of Harrison's phone

In addition to the Government's use of the cell site simulator being an unconstitutional search of Harrison's apartment, it is also an unconstitutional search of Harrison's phone, which is also protected under the Fourth Amendment as an "effect." *Cf. United States v. Jones*, 132 S. Ct. 945, 946 (2012) (stating that a vehicle is an "effect" under the Fourth Amendment).

The Supreme Court addressed a similar issue in *United States v. Jones* and held that the Government's attachment of a GPS tracking device to the defendant's vehicle and its use of that device to monitor the vehicle's movements constituted a search under the Fourth Amendment, and, accordingly, a warrant was required. *See id.* at 949. The Court addressed the issue under the theory of a Governmental trespass (a "physical intrusion") onto the defendant's effect (the vehicle).[18] *Id.* Although the use of the cell site simulator here is an electronic, rather than a physical, intrusion, the Court made no references that would differentiate between the two. Because that case did not require an analysis regarding electronic intrusion, the Court purposefully left the question at issue in this case open, but it also suggested that "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy[.]" *Id.* at 954.

Here, the Government searched Harrison's phone with the cell site simulator when it presumably[19] sent signals to Harrison's phone and forced the phone to respond to the fake cell tower. This is very different from using cell tower records because the person already knows (or should know) that the cellular service provider is obtaining signals when the phone is on. In contrast, with the cell site simulator, the person has no idea that the Government is obtaining signals (and other information) or that the signals are occurring as a direct result of Government's actions. Thus, the switch from inactive monitoring (*i.e.,* obtaining records) to

[18] The expectation-of-privacy line of Supreme Court cases also supports the conclusion that the cell site simulator search is a trespass. For example, in *Katz v. United States*, 389 U.S. 347 (1967), the Court found a violation of the Fourth Amendment where the Government was eavesdropping on a conversation in a public telephone booth.

[19] This operates on the assumption that the technology used in this case is similar to the cell site simulator described in the DOJ's Electronic Surveillance Manual, discussed *supra*. Undersigned counsel is unaware of how Harrison's phone was actually located, technologically, as explained in Defendant's Motion to Compel.

active monitoring (*i.e.*, using the cell site simulator), like the switch from traditional visual surveillance to GPS tracking in *Jones*, is a search, which requires a warrant.

Further, in *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court unanimously enunciated that a phone is more similar to a house, like in *Karo*, than a car, like in *Jones*, and held that a search of a phone requires a warrant. It explained, "[i]ndeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home: it also contains a broad array of private information never found in a home in any form—unless the phone is." *Id.* at 2491. Therefore, *Riley* offers even more support for the fact that the Government's use of the cell site simulator is a search of the phone that requires a warrant. *See id.* at 2495 ("Our answer to the question of what the police must do before searching a cell phone . . . is accordingly simple—get a warrant.").

c. The search of Harrison's person

Finally, the Government's use of the cell site simulator constitutes a search of Harrison's person under the Fourth Amendment because, in this modern era, a phone is essentially an extension of a person's body.

As explained *supra*, the Supreme Court's analysis in *Riley* strongly supports this view. For example, the Court stated that "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of the human anatomy." *Id.* at 2484. To be sure, the Court cited a study that found that "nearly three-quarters of smartphone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Id.* at 2490.

Thus, it is by no means illogical to analogize tracking a phone to tracking the movement of someone's arm, or searching a phone to searching the contents of someone's mind. By using devices like cell site simulators, the Government is able to tell where the phone is within two meters (approximately six feet) of its actual location. *See supra* note 13. If the phone is usually within five feet of the person, then the Government instantly has about an eleven-foot diameter of where an individual is at all times. That is very close to actually monitoring (searching) an individual.

This becomes even more problematic if, say, some persons were having a meeting in a house. Now the Government may be able to tell who is at the meeting by reading the phones' IMSI signals, what is being discussed by reading the content of messages, who left the room and what time they left, etc. The potential for intrusion of this type of technology is unbounded—and all the more reason why this Court must require a warrant that specifically authorizes it.

B. Because The Use of The Cell Site Simulator Violated The Fourth Amendment, The Evidence Gathered As a Result Must Be Suppressed.

Because there was a Fourth Amendment violation, the exclusionary rule applies to bar the introduction of the evidence obtained as a result therefrom. The exclusionary rule fashioned in *Weeks v. United States*, 232 U.S. 383 (1914), and *Mapp v. Ohio*, 367 U.S. 643 (1961), "excludes from a criminal trial any evidence seized from the defendant in violation of his Fourth Amendment rights. Fruits of such evidence are excluded as well." *Alderman v. United States*, 394 U.S. 165, 171 (1969).

Here, the searches of Harrison's apartment, person, and phone were in violation of the Fourth Amendment, as they were conducted without a warrant, and no exception to the warrant requirement applies. Therefore, the exclusionary rule applies and operates to exclude any such evidence and fruits of such evidence from Harrison's criminal trial. *See id.*; *see also, e.g., Karo*,

468 U.S. at 705 (stating that, because there was no warrant, the information gained from the beeper/GPS tracking device was "therefore inadmissible against those with privacy interests in the house").

IV. CONCLUSION

For the foregoing reasons, Defendant Robert Harrison respectfully requests that this Honorable Court grant this Motion to Suppress and exclude that all evidence seized as a result of the unconstitutional search, and evidence derived therefrom, and for such other and further relief as this Court deems appropriate.

Respectfully Submitted,

_____/s/_____
C. Justin Brown
Kasha Leese
LAW OFFICE OF C. JUSTIN BROWN
231 East Baltimore Street, Suite 1102
Baltimore, Maryland 21202
Tel: (410) 244-5444
Fax: (410) 934-3208
brown@cjbrownlaw.com

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 10th day of October, 2014, a copy of the foregoing Motion was sent to each of the parties via CM/ECF.

_____/s/_____
C. Justin Brown