

---

Appeal No. 15-CF-322

---

DISTRICT OF COLUMBIA COURT OF APPEALS

PRINCE JONES,

Appellant,

v.

UNITED STATES OF AMERICA,

Appellee.

---

Appeal from the Superior Court of the District of Columbia  
Criminal Division

---

BRIEF FOR APPELLANT

---

SAMIA FAM

JACLYN FRANKFURT

\*STEFANIE SCHNEIDER

PUBLIC DEFENDER SERVICE  
633 Indiana Avenue, NW  
Washington, DC 20004  
(202) 628-1200

\*Counsel for Oral Argument

## DISCLOSURE STATEMENT

Appellant Prince Jones was represented at trial by James Whitehead and Jullian Harris of the Public Defender Service for the District of Columbia (“PDS”). The government was represented by Jodi Lazarus and Uma Amuluru. The Honorable Jennifer Anderson presided over the trial. On appeal, Mr. Jones is represented by Samia Fam, Jaclyn Frankfurt, and Stefanie Schneider of PDS.

TABLE OF CONTENTS

	<u>Page</u>
TABLE OF AUTHORITIES .....	ii
ISSUE PRESENTED.....	1
ARGUMENT.....	24
I. THE GOVERNMENT’S WARRANTLESS USE OF A CELL SITE SIMULATOR TO TRACK THE PRECISE LOCATION OF MR. JONES’S CELL PHONE WAS AN ILLEGAL SEARCH IN VIOLATION OF THE FOURTH AMENDMENT.....	24
A. THE USE OF A CELL SITE SIMULATOR ON MR. JONES’S PHONE CONSTITUTED A TRESPASS UNDER <i>JONES V. UNITED STATES</i> .....	26
B. THE USE OF A CELL SITE SIMULATOR VIOLATED REASONABLE EXPECTATIONS OF PRIVACY UNDER <i>KATZ V. UNITED STATES</i> .....	31
C. CONTRARY TO THE TRIAL COURT’S RULING, THE INEVITABLE DISCOVERY DOCTRINE DOES NOT APPLY.....	37
D. THE FRUITS OF THE ILLEGAL SEARCH SHOULD HAVE BEEN SUPPRESSED.....	40
E. THE TRIAL COURT’S ERROR IN FAILING TO SUPPRESS THE FRUITS OF THE ILLEGAL SEARCH WAS NOT HARMLESS.....	48
CONCLUSION.....	50

## TABLE OF AUTHORITIES

	<u>Page</u>
<b>Cases</b>	
<i>America Online, Inc. v. LCGM, Inc.</i> , 46 F. Supp. 2d 444 (E.D. Va. 1998).....	28
<i>Andrews v. United States</i> , 922 A.2d 449 (D.C. 2007) .....	49
<i>In re Application of United States for Historical Cell Site Data</i> , 724 F.3d 600 (5th Cir. 2013).....	36, 37
<i>Brown v. Illinois</i> , 422 U.S. 590 (1975).....	42
<i>Bryant v. United States</i> , 599 A.2d 1107 (D.C. 1991) .....	47
<i>Burleson v. United States</i> , 306 A.2d 659 (D.C. 1973).....	49
<i>California v. Ciraolo</i> , 476 U.S. 207 (1986).....	32
<i>Chapman v. California</i> , 386 U.S. 18 (1967).....	48, 49
<i>Commonwealth v. Augustine</i> , 4 N.E.3d 846 (Mass. 2014) .....	33, 36, 37
<i>CompuServe, Inc. v. Cyber Promotions, Inc.</i> , 962 F. Supp. 1015 (S.D. Ohio 1997) .....	28
<i>Douglas-Bey v. United States</i> , 490 A.2d 1137 (D.C. 1985) .....	39
<i>eBay, Inc. v. Bidder’s Edge</i> , 100 F. Supp. 2d 1058 (N.D. Cal. 2000) .....	29
* <i>Ellis v. United States</i> , 941 A.2d 1042 (D.C. 2008).....	48, 49, 50
<i>Florida v. Jardines</i> , 133 S. Ct. 1409 (2013).....	27
<i>Gordon v. United States</i> , 120 A.3d 73 (D.C. 2015).....	41, 42
<i>Hayes v. Florida</i> , 470 U.S. 811 (1985).....	48
<i>Hicks v. United States</i> , 730 A.2d 657 (D.C. 1999).....	38, 39, 40
<i>Ingram v. United States</i> , 592 A.2d 992 (D.C. 1991) .....	49
* <i>Katz v. United States</i> , 389 U.S. 347 (1967) .....	<i>passim</i>
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	32
<i>McFerguson v. United States</i> , 770 A.2d 66 (D.C. 2001).....	39
<i>Missouri v. McNeely</i> , 133 S. Ct. 1552 (2013) .....	38

<i>*Murray v. United States</i> , 487 U.S. 533 (1988) .....	41, 44, 48
<i>Pearson v. Dodd</i> , 410 F.2d 701 (D.C. Cir. 1969).....	27
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978).....	30
<i>*Register.com, Inc. v. Verio, Inc.</i> , 356 F.3d 393 (2d Cir. 2004).....	29
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014).....	12, 25, 30, 33
<i>Silverman v. United States</i> , 365 U.S. 505 (1961) .....	30, 31
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	32, 36
<i>*State v. Earls</i> , 70 A.3d 630 (N.J. 2013).....	<i>passim</i>
<i>State v. Kerron Andrews</i> , Case No. 114149007 (Balt. City Cir. Ct. – Crim. 2015), <i>appeal docketed</i> , No. 1496 (Md. Ct. Spec. App. Sept. 3, 2015).....	25
<i>State v. Perry</i> , 776 S.E.2d 528 (N.C. Ct. App. 2015).....	36
<i>State v. Tate</i> , 849 N.W.2d 798 (Wis. 2014).....	24, 29
<i>Thrifty-Tel, Inc. v. Bezenek</i> , 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996) .....	28
<i>*Tracey v. State</i> , 152 So. 3d 504 (Fla. 2014) .....	<i>passim</i>
<i>United States v. Allen</i> , 436 A.2d 1303 (D.C. 1981).....	38, 42
<i>*United States v. Ceccolini</i> , 435 U.S. 268 (1978) .....	45, 46, 47
<i>United States v. Crews</i> , 445 U.S. 463 (1980) .....	47
<i>United States v. Davis</i> , 785 F.3d 498 (11th Cir. 2015) (en banc).....	36, 43
<i>United States v. Gooding</i> , 695 F.2d 78 (4th Cir. 1982).....	43
<i>United States v. Heath</i> , 455 F.3d 52 (2d Cir. 2006) .....	38
<i>United States v. Ienco</i> , 182 F.3d 517 (7th Cir. 1999).....	46
<i>*United States v. Jones</i> , 132 S. Ct. 945 (2012) .....	<i>passim</i>
<i>United States v. Knotts</i> , 460 U.S. 276 (1983).....	36
<i>United States v. Miller</i> , 821 F.2d 546 (11th Cir. 1987).....	43
<i>United States v. Rubalcava-Montoya</i> , 597 F.2d 140 (9th Cir. 1979) .....	45, 46
<i>United States v. Skinner</i> , 690 F.3d 772 (6th Cir. 2012).....	36

<i>United States v. Washington</i> , 490 F.3d 765 (9th Cir. 2007).....	43
<i>Wilson v. United States</i> , 102 A.3d 751 (D.C. 2014).....	41
* <i>Wong Sun v. United States</i> , 371 U.S. 471 (1963).....	41, 42
<b>Statutes</b>	
18 U.S.C. § 2703(c).....	43
18 U.S.C. § 3121(d).....	41
D.C. Code § 22-1810 (2001 ed.).....	1
D.C. Code § 22-2001 (2001 ed.).....	1
D.C. Code § 22-2801 (2001 ed.).....	1
D.C. Code § 22-4502 (2001 ed.).....	1
D.C. Code §§ 22-3002(a)(1) and (2) (2001 ed.).....	1
D.C. Code § 22-3020(a)(5) (2001 ed.).....	1
D.C. Code § 22-3020(a)(6) (2001 ed.).....	1
<b>Other Authorities</b>	
DOJ Policy Guidance: Cell Site Simulator Technology, Sept. 3, 2015.....	35
DHS Policy Directive 047-02, Oct. 19, 2015.....	35
Justin Fenton, <i>Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods</i> , Baltimore Sun (Nov. 17, 2014).....	25, 34
Letter from Patrick Leahy and Charles Grassley, U.S. Senators, to Eric Holder, Att’y Gen., and Jeh Johnson, Sec’y of Homeland Security (Dec. 23, 2014).....	35
Matt Richell, <i>A Police Gadget Tracks Phones? Shhh! It’s Secret</i> , N.Y. Times (Mar. 15, 2015).....	25, 34
Stephanie K. Pell & Christopher Soghoian, <i>Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy</i> , 28 Harv. J.L. & Tech. 1, 14-15 (Fall 2014).....	24, 25, 34
Prosser & Keeton, Torts (5th ed. 1984).....	28

R. Craig Curtis et al., <i>Using Technology the Founders Never Dreamed Of: Cell Phones as Tracking Devices and the Fourth Amendment</i> , 4 U. Denv. Crim. L. Rev. 61, 63 (2014). .....	35
Restatement (Second) of Torts (1965).....	27, 28
Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. Act (1st Sess. 2015) .....	35
6 Wayne R. LaFave, <i>Search &amp; Seizure</i> § 11.4(a), (4th ed. 2004) .....	39

\* An asterisk denotes an authority upon which the appellant chiefly relies.

## ISSUE PRESENTED

Whether the government's warrantless use of a cell site simulator to disable Mr. Jones's cell phone, convert it into a tracking device, and pinpoint its precise location was an illegal search in violation of the Fourth Amendment.

## STATEMENT OF THE CASE

The charges in this case arose from the alleged sexual assaults of Tamara Shipp and Stephanie Hawkins-Ross, and the corresponding robberies of Ms. Shipp, Ms. Hawkins-Ross, and Christina Hancock. On January 29, 2014, the grand jury charged Prince Jones with two counts of first-degree sexual abuse while armed (two or more victims), in violation of D.C. Code §§ 22-3002(a)(1) and (2), -3020(a)(5), -3020(a)(6), -4502 (2001 ed.); two counts of kidnapping while armed, in violation of D.C. Code §§ 22-2001, -4502 (2001 ed.); four counts of robbery while armed, in violation of D.C. Code §§ 22-2801, 4502 (2001 ed.); and one count of threats, in violation of D.C. Code § 22-1810 (2001 ed.). R. 25. Following pretrial motions, a jury trial commenced on October 29, 2014, before the Honorable Jennifer Anderson. On November 13, 2014, the jury convicted Mr. Jones of all charges. 11/13/14 at 12-14. On February 27, 2015, the trial court sentenced Mr. Jones to 792 months of incarceration, to be followed by lifetime supervised release. 2/27/15 at 31-33; R. 71. Mr. Jones filed a timely notice of appeal. R. 72.

## STATEMENT OF FACTS

### **I. Overview**

The charges in this case stem from the alleged sexual assaults and robberies of Tamara Shipp and Stephanie Hawkins-Ross, escorts who advertised their services on Backpage.com and were allegedly assaulted by their client. At approximately 1:00 a.m. on October 9, 2013, Ms. Shipp and her cousin Christina Hancock reported that a man had forced Ms. Shipp to perform oral sex at knifepoint in an apartment building on B Street, SE, and then robbed Ms. Shipp and



Ms. Hancock of their cell phones, money, and Ms. Shipp's purse. Two days later, in the early morning hours of October 11, 2013, Ms. Hawkins-Ross reported that she, too, had been forced to perform oral sex at knifepoint and robbed at the same location. The assailant allegedly took her money, two cell phones, cell phone charger, bank cards, identification cards, and Metro cards.

Because both Ms. Shipp and Ms. Hawkins-Ross were contacted by phone in response to their advertisements, the police obtained their call records and discovered that the same phone number—240-313-5281—had called both women. Without obtaining a warrant, the police obtained from AT&T the cell phone records associated with this suspect phone number. However, because it was a prepaid cell phone, there was no identification information about the phone's owner. The police proceeded to track the location of this AT&T phone and Ms. Shipp's Sprint phone using information provided by the cell phone companies about the cell towers with which the phones were communicating. Using this cell site location information ("CSLI"), the police concluded that the two phones were somewhere in the general vicinity of the Minnesota Avenue Metro station, but they were unable to determine the precise location of either phone.

Without getting a warrant, the police then used proprietary law enforcement technology, generically known as a cell site simulator, to pinpoint the location of the suspect phone. By simulating an AT&T cell tower, the cell site simulator forced Mr. Jones's phone to disconnect from the AT&T network and communicate with the cell site simulator. As a result, Mr. Jones's phone was not operational during this time period. He was unable to make or receive calls, and his phone dropped a call mid-conversation. The cell site simulator provided the police the precise direction and distance of Mr. Jones's phone and led them to his parked red Saturn in the 4000 block of Minnesota Avenue, N.E. As a direct result of the stop of Mr. Jones, the police recovered Mr. Jones's cell phones; the cell phones of all three complainants; Ms. Shipp's pink

and green purse; and Ms. Hawkins-Ross's Smart Trip cards. They also obtained a photograph of Mr. Jones's groin, a DNA sample, a statement, Ms. Hawkins-Ross's identification, extraction reports from the phones, and the unwilling testimony of Mr. Jones's girlfriend, Ms. Williams.

Mr. Jones filed a motion to suppress the fruits of the warrantless use of a cell site simulator to track his phone. The trial judge denied the motion on inevitable discovery grounds. Without deciding whether use of a cell site simulator constituted a search under the Fourth Amendment, she erroneously found no Fourth Amendment violation because she believed that the police could have discovered Mr. Jones's location by using the cell site simulator on the complainant's phone. Because the warrantless use of a cell site simulator violated Mr. Jones's Fourth Amendment rights, the inevitable discovery doctrine did not apply, and nearly all of the evidence was the fruit of the illegal search, Mr. Jones's convictions must be reversed.

## **II. The Suppression Hearing**

The defense initially filed a motion to suppress arguing that there was no probable cause or reasonable suspicion to detain and arrest Mr. Jones. R. 24. After learning through discovery that the police had tracked the location of Mr. Jones's phone—first by obtaining cell site location information from AT&T, and second by using a cell site simulator to pinpoint his location in a red Saturn on the 4000 block of Minnesota Avenue—Mr. Jones filed a supplemental motion to suppress asserting that the warrantless tracking of his cell phone violated the Fourth Amendment. R. 49.<sup>1</sup> The government presented two witnesses at an evidentiary hearing—Sergeant Todd Perkins and Detective Rachel Pulliam of the Metropolitan Police Department (MPD). In response, the defense presented the expert testimony of Ben Levitan.

---

<sup>1</sup> On appeal, Mr. Jones challenges only the warrantless use of the cell site simulator.

A. Cell Phone Tracking of Mr. Jones's Phone and the Complainant's Phone Through Cell Site Location Information Provided by Cell Phone Companies

Sergeant Perkins, an MPD officer in the technical services unit, began his shift at 6:30 or 7:00 a.m. on October 11, 2013, and “[w]ithin an hour” was assigned the present case. 10/17/14 at 9, 14. Sergeant Perkins explained that he first obtained the cell phone records of Ms. Shipp and Ms. Hawkins-Ross and determined that both women had been contacted by a phone with the number 240-313-5281—a number provided by AT&T. *Id.* at 10-12. He decided to track the location of this phone. *Id.* at 11. Sergeant Perkins testified that although MPD’s general practice was to get a warrant before tracking a suspect’s phone, he failed to get any type of court order in this case. *Id.* at 13-14. Instead, he declared exigent circumstances to AT&T. *Id.*

AT&T first provided the phone’s subscriber information, but because it was a prepaid phone, there was no information about the owner’s identity. *Id.* at 17. Sergeant Perkins then began receiving information about the location of the phone in fifteen-minute intervals. *Id.* at 16-18, 80. Because the phone’s GPS function was turned off, it was not “true GPS” but rather an estimated area where the phone was likely to be based on the location of the cell phone tower with which it was communicating. *Id.* at 80. Specifically, AT&T provided the latitude, longitude, and 120-degree sector of the cell tower as well as a several-hundred-meter estimate of the distance the tower’s signal was likely to travel. *Id.* at 80-81. Using this information, Sergeant Perkins plotted the estimated location of the phone on a map. *Id.* at 17. Sergeant Perkins simultaneously tracked the location of Ms. Shipp’s Sprint phone using Sprint’s law enforcement website and got updates in five-minute intervals. *Id.* at 21, 26.<sup>2</sup> True GPS was similarly unavailable, so Sprint provided the latitude and longitude of the cell tower and

---

<sup>2</sup> Ms. Hawkins-Ross had a Sprint phone that was turned off and could not be tracked. *Id.* at 26. She also had a Verizon phone, but because Verizon only provides location information when a call is placed or received, the information was less useful for investigative purposes. *Id.*

represented the likely location of the phone as a shaded circle on a map with the cell tower in the center. *Id.* at 22, 91-92.

Sergeant Perkins testified that by tracking the two phones simultaneously, he concluded that they were traveling in the same general direction, as if they were together. *Id.* at 26-27. He explained that Government Exhibit 3 was a map of the estimated location of the complainant's Sprint phone at 11:20 a.m. *Id.* at 31-32. It reflected a cell tower east of Kenilworth Avenue, NE, and just north of Benning Road, NE. App'x F. Government Exhibit 5 was a map of the suspect AT&T phone between 11:23 and 11:31 a.m. 10/17/14 at 39. It reflected a cell tower east of Kenilworth Avenue, NE, and south of Benning Avenue, NE. App'x G.<sup>3</sup> According to Sergeant Perkins, both maps suggested that the phones were in the general vicinity of the Minnesota Avenue Metro, so he and his team proceeded to that area. 10/17/14 at 41.

**B. MPD's Use of a Cell Site Simulator to Pinpoint Mr. Jones's Location**

Sergeant Perkins testified that he next used a cell site simulator to get a more precise location. *Id.* at 42. Although not an expert, Sergeant Perkins described a cell site simulator as specialized equipment that can locate a phone once it is in the general vicinity of the phone. *Id.* at 89. He explained that cell phones are radios and are always transmitting and receiving information from a cell tower, even when not in use. *Id.* at 44, 97, 100. When MPD wants to locate a phone, it enters identifying information such as an international mobile subscriber identification number (IMSI) into the cell site simulator. *Id.* at 97. The officers then drive around the target area while the cell site simulator "listen[s]" for the frequency of the target phone. *Id.* at 44, 97, 100. After confirming that the phone is present, the cell site simulator determines the phone's location based on its direction and signal strength. *Id.* at 98. It provides

---

<sup>3</sup> A motion to supplement the record with Government Exhibits 3 and 5 has been filed with the Court.

the officers a precise direction on a 360-degree antenna and uses the signal strength to estimate the distance of the phone. *Id.* at 98-99. Sergeant Perkins testified that this technology works only when it is close to the target phone, which is why MPD initially obtained information from AT&T and Sprint to determine the general geographic area of the phones. *Id.* at 89-90.

Sergeant Perkins explained that when a cell site simulator is being used on a particular phone, it prevents communication between the target phone and the network's cell tower. *Id.* at 43-44, 103. It "grabs [the phone] and holds on to it," at which point the phone can no longer contact the tower. *Id.* at 44. As he described it, the cell site simulator "takes over the position . . . of the cell tower itself" and "takes the phone's transmissions." *Id.* at 99. Accordingly, the phone is unable to make or receive calls because it cannot communicate with the tower. *See id.* at 43-44. Sergeant Perkins further explained that no action on the part of the user—*e.g.*, a phone call, text, or email—is necessary for the cell site simulator to determine the phone's location; the phone merely needs to be powered on. *Id.* at 100.

Sergeant Perkins testified that he tracked one of the two cell phones with the cell site simulator, but he could not remember which one. *Id.* at 42, 97. He explained that a cell site simulator can only locate one phone at a time and although MPD had two police trucks with cell site simulators, only one of the two was operational. *Id.* at 65-66, 97. No records documented which of the two phones was tracked. *Id.* at 69. Despite his lack of memory, Sergeant Perkins speculated that he likely used the cell site simulator on the complainant's Sprint phone. *Id.* at 42. His primary basis for this belief was a single "location error" on the Sprint records which showed that at 11:19 a.m., Sprint was unable to determine where the phone was—*i.e.*, what tower it was communicating with. *Id.* at 43. Sergeant Perkins hypothesized that the reason for the failure was that the cell site simulator was tracking the Sprint phone and therefore the phone was unable to

contact the Sprint tower. *Id.* He also noted a request for the AT&T phone's IMSI on the radio run, but he did not recall getting a response. *Id.* at 121. He observed that without the IMSI, it would have been impossible to use the cell site simulator on the AT&T phone. *Id.* Both of these hypotheses were subsequently called into question by defense expert Ben Levitan, and the trial court ultimately ruled that the government had not met its burden to show that the government tracked the complainant's phone. *See infra* pp. 9-10; 13-14.

Sergeant Perkins testified that he used the cell site simulator for approximately 30-45 minutes before locating Mr. Jones on the 4000 block of Minnesota Avenue, NE. *Id.* at 90, 95. He entered the block because he was getting "hits for the phone." *Id.* at 48. He described the 4000 block of Minnesota Avenue as a large block with a number of businesses, including a strip mall, convenience stores, and Auto Zone, as well as a government building and Metro station. *Id.* at 94. Sergeant Perkins acknowledged that the area would have been busy between 11:00 and 11:30 a.m. on a Friday morning, the time of the stop. *Id.* at 95. Sergeant Perkins testified that as he drove southbound on the 4000 block of Minnesota Avenue, the directional arrow on the cell site simulator pointed towards a parked, occupied red Saturn. *Id.* at 48-49, 103. One of the passengers was a tall, thin, black male with a scruffy beard, and he was holding a flip phone, which was consistent with the lookout. *Id.* at 50-51, 107. The officers approached the car to question its occupants—Appellant Prince Jones and Nora Williams. 10/24/14 at 16, 21.

### C. The Stop of Mr. Jones and the Resulting Evidence

Sergeant Perkins testified that Officers Regan and Overmyer approached the car, advised Mr. Jones that they were investigating a criminal matter, and asked him to step out. 10/17/14 at 51-52. Mr. Jones complied, leaving the flip phone in the car. *Id.* at 52, 54-55. Officer Overmyer observed a pocket knife protruding from Mr. Jones's pocket, retrieved it, and placed Mr. Jones in handcuffs. *Id.* at 52-54. Sergeant Perkins testified that he tried calling the phone

numbers of the stolen phones, and the flip phone in Mr. Jones's car rang. *Id.* at 55. Shortly thereafter, Detective Elbert Griffin and Detective Rachel Pulliam of the sexual assault unit arrived. 10/24/14 at 15. When Detective Griffin asked Mr. Jones for his biographical information, he provided the address of the second complainant—Ms. Hawkins-Ross. *Id.* at 19.<sup>4</sup>

Detective Griffin and Detective Pulliam asked to speak with Ms. Williams in the back of their police vehicle because it was raining. *Id.* at 22. Detective Pulliam testified that while they were talking, phones in Ms. Williams's purse kept ringing. *Id.* at 23. Detective Griffin then asked Ms. Williams for consent to search her purse. *Id.* He explained that Mr. Jones was going to be arrested and that he believed there might be evidence in her purse. *Id.* at 25. He advised her that she could consent to the search, *or* the police would take her purse into custody and get a search warrant. *Id.* Ms. Williams signed a consent form. *Id.* at 25-26.

The police recovered four phones from Ms. Williams's purse: a black iPhone that Ms. Williams identified as Mr. Jones's<sup>5</sup>; Ms. Williams's Samsung Galaxy phone; Ms. Hawkins-Ross's Samsung Galaxy phone; and Ms. Hancock's white iPhone. *Id.* at 26-29. Ms. Hawkins-Ross's cell phone case was on Ms. Williams's phone, and vice versa. *Id.* at 28-29. The police towed Mr. Jones's car to the mobile crime unit, got a search warrant for the car, and recovered Ms. Hawkins-Ross's Verizon flip phone, Ms. Shipp's HTC phone, and Ms. Shipp's purse. *Id.* at 29-30. The police got warrants to search the contents of the recovered phones. *Id.* at 30-31.

After the stop, the detectives also conducted photo arrays with the three complainants.

---

<sup>4</sup> At the suppression hearing, Ms. Shipp was referred to as Complainant 1, Ms. Hawkins-Ross as Complainant 2, and Ms. Hancock as Complainant 3. *See* 10/24/14 at 42-43. For clarity, the complainants are referred to by their names throughout the brief.

<sup>5</sup> This phone was subsequently identified as having the 240-313-5281 phone number, which was listed in both Ms. Shipp's and Ms. Hawkins-Ross's phone records. 10/24/14 at 24.

*Id.* at 31. Ms. Hawkins-Ross was the only complainant to identify Mr. Jones. She selected his photograph and said, “[I]t kind of looks like him.” *Id.* at 33-34.

D. Preliminary Ruling and Motion to Reconsider

On October 24, 2014, the trial court found that the government had shown by a preponderance of the evidence that it used the cell site simulator to track the complainant’s phone, not Mr. Jones’s phone. 10/24/14 at 101-02. Accordingly, the court ruled that Mr. Jones had no standing to raise a Fourth Amendment challenge and denied his motion to suppress on that basis. *Id.* at 102. On October 27, 2014, the defense filed a Motion to Reconsider. R. 53. In the alternative, it asked the Court to reopen the motions hearing for presentation of expert testimony. *Id.* at 5. The trial court allowed the defense to present expert testimony.

E. Defense Expert Witness Ben Levitan

The defense called Ben Levitan, an expert in cell phone networks and systems forensics, to challenge the factual bases of Sergeant Perkins’s belief that he tracked the complainant’s Sprint phone. 10/29/14 at 223. Mr. Levitan explained that cell phones interact with the network providers through a two-way radio communication between the cell phone and the cell tower. *Id.* at 226. Whenever a cell phone is on, it connects to the cell tower with the strongest signal, which is generally the closest cell tower. *Id.* When a cell phone and tower are connected, they exchange information, including location. *Id.* at 226-27. However, if another tower, such as a cell site simulator, has a stronger signal, the cell phone will connect to the cell site simulator and will not respond to the network. *Id.* at 228. When that occurs, all calls will fail. *Id.* at 230.

Mr. Levitan reviewed the records for the complainant’s Sprint phone. *Id.* at 230-31. He explained that the records reflected “pings”—requests by the cell phone network to a cell phone to return its location. *Id.* at 231. The records showed that between 11:19 a.m. and 12:41 p.m.



EST, there were six requests for the cell phone's location from the Sprint network, and each time the request was successful—*i.e.*, the phone responded with a location. *Id.* at 233. However, at 11:19 a.m. EST, the request for location failed. *Id.* Mr. Levitan opined that the phone's failure to connect with the network was due to one of five reasons: (1) the phone was off; (2) the phone was in an area of poor coverage; (3) there was a line of sight problem—*i.e.*, something blocked the signal between the phone and tower; (4) there was a high degree of interference such as electromagnetic noise; or (5) the phone responded to a different tower such as a cell site simulator. *Id.* at 228, 237. He stated that there was no way to tell why the phone did not respond to the Sprint network that one time. *Id.* at 237.

Mr. Levitan also reviewed the call detail records, or SCAMP, associated with Mr. Jones's AT&T phone. He observed that the phone attempted seven calls between 11:23 a.m. and 11:31 a.m. EST, and all seven failed. *Id.* at 239-40. Mr. Levitan reviewed the subscriber information for Mr. Jones's phone, which Sergeant Perkins received from AT&T, and confirmed that it listed the phone's IMSI. *Id.* at 243. Additionally, he reviewed extraction reports which contained text messages found on Mr. Jones's phone. *Id.* at 247-48. He testified that at 11:25 a.m. EST, there was an outgoing text message that said, "Our call dropped." *Id.* at 249. He further testified that six of the seven failed calls were to this same number, immediately after a successful 14-minute call to that number between 11:09 a.m. and 11:23 a.m. EST. *Id.* at 250, 266-67.

Following Mr. Levitan's testimony, the prosecutor disclosed that she had listened to the radio run again, and Sergeant Perkins had asked about a password for the AT&T site which he could have used to retrieve the IMSI. *Id.* at 286. Although no one gave him a specific password, he was advised that "it's the same as on the email," or words to that effect. *Id.* at 286-87.

#### F. The Government's Argument

The prosecutor conceded that “there is ambiguity as to which phone was being used” by the cell site simulator. *Id.* at 288. As she told the court, “[t]he government doesn’t have enough evidence at this point to put before the Court that it was definitely using one phone or the other.” *Id.* at 301. She had previously acknowledged that whether warrantless cell phone tracking violates the Fourth Amendment “is a complicated legal issue and that there is [a] divide within the courts.” 10/24/14 at 81. Accordingly, rather than addressing whether the Fourth Amendment required the government to get a warrant before using the cell site simulator, she asked the Court to rule on one of several alternative grounds. 10/29/14 at 288-290, 301. First, she argued inevitable discovery, asserting that “inevitably they would have found him either with the Sprint or the AT&T phone.” *Id.* at 288. She argued that “[w]hen there is a separate, lawful way you could have gotten to the same thing, suppression just isn’t the appropriate remedy because suppression is disfavored.” *Id.* at 288-89. She further maintained that the cell site simulator “is going to work the same way on either phone.” *Id.* at 295. Second, she argued that a cell site simulator is a “pen register” under the Patriot Act and suppression is not a remedy under the statute. *Id.* at 289. Finally, she argued that there were exigent circumstances. *Id.*<sup>6</sup>

#### G. The Defense Argument

Defense counsel argued that the evidence showed that the government used the cell site simulator on Mr. Jones’s AT&T phone. He noted that there was only a single failed communication on the Sprint phone at 11:19 a.m., but a series of failed AT&T calls between 11:23 a.m. and 11:31 a.m. as well as an 11:25 a.m. text message from Mr. Jones that his call had

---

<sup>6</sup> The government made essentially the same arguments on October 24, 2013, and in its opposition to Mr. Jones’s supplemental motion to suppress. *See* 10/24/14 at 81-83; App’x C. A motion to supplement the record with this pleading has been filed with the Court.

dropped. 10/29/14 at 291-92. He argued that this evidence, in conjunction with Sergeant Perkins's request for the password to look up the IMSI for the AT&T phone, supported an inference that the government used the cell site simulator on Mr. Jones's phone. *Id.* at 293-94.

The defense had previously argued that the warrantless use of a cell site simulator to track the location of Mr. Jones's cell phone violated the Fourth Amendment. Citing *Katz v. United States*, 389 U.S. 347 (1967), *United States v. Jones*, 132 S. Ct. 945 (2012), and *Riley v. California*, 134 S. Ct. 2473 (2014), Mr. Jones argued in his Supplemental Motion to Suppress that he had a reasonable expectation of privacy in the real-time location of his cell phone and that the government "encroached upon a protected area" by "direct manipulation of Mr. Jones's cell phone through a tracking device." R. 49 at 4-5. He argued that the government "essentially hacked into the cell phone and forced transactions rather than collecting data based on overt use by Mr. Jones." *Id.* at 5. In his Second Supplemental Motion to Suppress, he cited *Tracey v. State*, 152 So. 3d 504 (Fla. 2014), in which the Florida Supreme Court held that individuals have a reasonable expectation of privacy in the location signals transmitted by their cell phones and that warrantless, real-time tracking violates the Fourth Amendment. R. 51 at 2-3.

Likewise, at the October 24, 2014 hearing, defense counsel argued that Mr. Jones had a reasonable expectation of privacy that the government would not use a cell site simulator to track the location of his phone. 10/24/14 at 96-97. Defense counsel noted that information about cell site simulators is not public and that the government "fought tooth and nail to not disclose certain particulars about the technology that was used in this case." *Id.* at 97.<sup>7</sup> He emphasized that cell site simulators can intercept the phone's radio transmissions even when the phone is not being used to make a call, text, or access data and that "nobody would ever believe that that would

---

<sup>7</sup> The government asserted law enforcement privilege and filed a motion in limine to limit disclosure about the particulars of the cell site simulator. R. 48.

happen nor would the public in general know anything about or expect that their radio transmissions are going to be intercepted by the police using some technology that we're all not aware of that's only within law enforcement, their purview." *Id.* at 97.

Argument on October 29, 2014 focused on the inevitable discovery doctrine. Defense counsel disputed that the doctrine applied and argued that it was speculative that police would have found Mr. Jones using the cell site simulator on the complainant's phone. He emphasized the "lack of evidence put on by the government . . . that there would have been success with the Sprint phone, with this particular cell site simulator." 10/29/14 at 307; *see also id.* at 303.<sup>8</sup>

#### H. Trial Court Ruling

The trial court reversed its prior finding that the police had tracked the complainant's phone. It found that the police got to the vicinity of the Minnesota Avenue Metro based on information provided by both Sprint and AT&T. *Id.* at 291. Once the police were in the general area, they used the cell site simulator, which is only capable of tracking one phone at a time. *Id.* The court observed that the evidence suggested that the police "probably" tracked Mr. Jones's AT&T phone with the cell site simulator. *Id.* at 305. In any event, the trial court found that "the government ha[d]n't met its burden" to show by a preponderance of the evidence that it had tracked the complainant's Sprint phone. *Id.* It explained:

---

<sup>8</sup> Defense counsel noted that if the single failed communication between Sprint and the complainant's phone at 11:19 a.m. was the result of the cell site simulator, then the evidence suggested that the cell site simulator was not working properly with the Sprint phone because none of the subsequent communications between Sprint and the complainant's phone failed. *Id.* at 302, 304-05, 308. Moreover, defense counsel argued that if the police had had success with the Sprint phone, they would have arrested Mr. Jones immediately. *Id.* at 300. Instead, he was not arrested until after 11:31 a.m., at which point there had been *seven* failed calls on Mr. Jones's phone and a text about a dropped call, which was consistent with the government using the cell site simulator on Mr. Jones's phone. *Id.* at 292, 296. Defense counsel argued that the court could infer that the police switched to the AT&T phone because the cell site simulator was not working properly with the complainant's Sprint phone. *Id.* at 298, 300.

All I conclude is that the government hasn't met its burden and so it could have been either phone so, therefore, it's the government's burden to prove, so on that basis, I'm going to conclude that they weren't entitled – that they haven't shown that they didn't use the defendant's phone.

*Id.* at 306.<sup>9</sup>

Despite finding that the police may have tracked Mr. Jones's phone, the trial court declined to address whether use of a cell site simulator is a search under the Fourth Amendment requiring a warrant. Instead, it denied the motion to suppress on inevitable discovery grounds:

[T]he sergeant's testimony was that when they were tracking the – when they were tracking the cell site information, before they got to the use of the cell site simulator, he testified that they were able to tell that the phones were together. So I do think that even if – even if they were using the AT&T phone on the cell site simulator, that had they switched over to use the Sprint – to use the Sprint number instead, so assuming for the moment that they used the AT&T number, then I think – I think they would have eventually gotten to the exact same place because the phones were together. And it's the same technology and you're just interfering with the cell – the cell connection. So I do think, in terms of inevitable discovery, they would have gotten to the exact same place, so the motion is denied.

*Id.* at 309-10.

The trial court further found that there were no exigent circumstances. *Id.* at 311. It noted that although there were three serious armed offenses, a lot of time elapsed before the cell phone tracking began. *Id.* at 310. The court emphasized that two separate police units worked the case—the technical services unit and sexual assault unit—and reasoned that “given the amount of time that had passed . . . the detectives could have been getting a warrant at the same time.” *Id.* at 310-11. “[G]iven the time lapse and given the structure of the way the police [were] working this particular case, I find that exigent circumstances did not exist.” *Id.* at 311.

---

<sup>9</sup> The trial court rejected the defense argument that the government was unsuccessful using the cell site simulator on the complainant's phone and switched to the defendant's phone. *Id.* at 306. It noted that Mr. Levitan described a multitude of reasons that would explain a single failure to communicate with the tower, and there was no testimony about switching phones. *Id.*

### III. The Trial

The government presented the testimony of Ms. Shipp, Ms. Hancock, and Ms. Hawkins-Ross, who claimed to have been sexually assaulted and robbed by an unknown man who responded to an advertisement for escort services. The government sought to corroborate their accounts and to connect Mr. Jones to the alleged crimes through evidence recovered as the fruit of the illegal cell site simulator search. The defense theory was that the sexual encounters were consensual and that the robberies were fabricated. Mr. Jones did not testify at trial.

#### A. The October 9, 2013 Incident – Tamara Shipp and Christina Hancock

Ms. Shipp testified that at approximately 10:00 p.m. on October 8, 2013, shortly after picking up her cousin Ms. Hancock in Gaithersburg, she posted an advertisement for escort services on Backpage.com. 10/30/14 at 51, 54-55, 95-96. The advertisement, captioned “Tall Thirst Quencher,” contained a photograph, her stage name, and a phone number. *Id.* at 52-53. Although Ms. Shipp had previously performed sexual acts for money, her practice was to list only her name and number and negotiate a price for her time so that she would not get in trouble. *Id.* at 51, 53, 97-99, 102, 105. A man responded, agreed to pay \$150 for thirty minutes, and texted an address on B Street, off of Benning Road. *Id.* at 54-55, 56, 100, 114.

When Ms. Shipp arrived at the apartment building, she saw a man wearing a grey sweatshirt with the hood up and string tied, grey jean shorts, and black tennis shoes. *Id.* at 58, 116. Ms. Hancock stayed in the car while Ms. Shipp approached the man. *Id.* at 58. According to Ms. Shipp, the man led her into the building and down a flight of stairs to a part of the building with no apartments. *Id.* at 58-59. Ms. Shipp testified that he then pushed her against the wall, pulled out a black and silver pocket knife, put it to her neck, and forced her to perform oral sex. *Id.* at 59, 65. Ms. Shipp observed that the man had no hair in his groin area. *Id.* at 66.

She testified that he did not initially wear a condom, but put one on prior to ejaculating. *Id.* at 66-67. She claimed that he did not pay her. *Id.* at 63. Instead, he held the knife to her neck and said, “I bet your dumb ass haven’t learned your lesson; probably going to go do the same dumb ass shit again.” *Id.* at 65-68.

Ms. Shipp testified that after oral sex, the man asked her how much money she had and she told him \$140. *Id.* at 67. According to Ms. Shipp, the man then walked her back to her van, holding the knife to her back the entire time. *Id.* at 67-68. Ms. Hancock testified that the man knocked on the passenger door and said, “[O]pen the fucking door.” 10/29/14 at 393-94. He then jumped in behind Ms. Hancock while Ms. Shipp walked around to the driver’s seat. *Id.* at 394. According to Ms. Hancock, the man said, “[D]on’t fucking look at me” and “I don’t want to hurt anyone.” *Id.* He then ordered the women, “[G]ive me everything you got.” *Id.* Ms. Shipp testified that the man took her money and her green and pink bag-type purse. 10/30/14 at 70-71. He also took both of their cell phones and demanded their pass codes. *Id.* at 70, 74, 75.

Ms. Hancock testified that after the man left, she insisted that she and Ms. Shipp go to the police. 10/29/14 at 403, 427. They flagged down Officer Kevin O’Malley on Benning Road and Ms. Shipp reported being robbed and forced to perform oral sex at knifepoint. *Id.* at 359; 10/30/14 at 75. Officer O’Malley requested the assistance of sexual assault detectives, but Ms. Shipp declined to wait for them to arrive. 10/29/14 at 360, 363. She did not go to the hospital that night, nor did she get examined by a sexual assault nurse examiner (SANE) the following day despite the detectives’ recommendation that she do so. 10/30/14 at 126-27.

Defense counsel pointed to several discrepancies and oddities in Ms. Shipp’s account of the evening. *See* 11/5/14 at 637-641. For example, she claimed that after picking up Ms. Hancock, but prior to meeting the man at B Street, she had an escort call in Oxon Hill, Maryland,

where she earned the \$140 that the assailant took from her. 10/30/14 at 67, 108-09, 151.

However, Ms. Hancock did not mention this stop in her testimony, and Luis DeJesus, an expert in cell detail and historical cell site records, analyzed Ms. Shipp and Ms. Hancock's cell phone records and testified that neither of their phones communicated with towers near Oxon Hill, Maryland, at that time. 11/5/14 at 502, 538-539. Similarly, it was strange that even though Ms. Shipp had previously performed oral sex for money and always required a condom, she claimed that she did not bring any with her when she went to meet this client, 10/30/14 at 117-18, and she did not go to the hospital after the incident, *id.* at 126-27. Defense counsel also emphasized the lack of Ms. Shipp's DNA on Mr. Jones's knife, notwithstanding her claim that there was a knife to her neck throughout the incident and expert testimony that epithelial cells with DNA could rub off under those circumstances. 11/4/14 at 318-19, 335-39; 11/5/14 at 642-43.

**B. The October 11, 2013 Incident – Stephanie Hawkins-Ross**

Ms. Hawkins-Ross also advertised escort services on Backpage.com. 11/3/14 at 33. Late on October 10, 2013, she posted an advertisement of herself wearing lingerie. *Id.* at 36, 101, 103-04. Like Ms. Shipp, she did not specify sexual acts and only listed her stage name and phone number. *Id.* at 36, 101, 103. Shortly after midnight, a man called her. *Id.* at 38-39. She told him she charged \$100 for thirty minutes and agreed to meet him in front of his apartment building on B Street, SE. *Id.* at 42, 106. Ms. Hawkins-Ross testified that the man had a beard, wore rectangular-shaped glasses, and had a hoodie over his head. *Id.* at 44-45. He entered the building without a key, and led her downstairs to the dimly lit laundry room. *Id.* at 43, 44.

Ms. Hawkins-Ross testified that she asked for her money, at which point the man put a knife to her neck. *Id.* at 46-47. He then forced her to take off her sweater, pull up her dress, and take off her boots. *Id.* at 48. He took the \$100 she had in her boots as well as the flip phone she



used for Backpage.com business. *Id.* at 49, 52, 58. Ms. Hawkins-Ross testified that the man forced her to her knees, made her perform oral sex without a condom, and ejaculated in her mouth. *Id.* at 50-51. Ms. Hawkins-Ross testified that after oral sex, the man asked if there was anyone in her car and said he would kill her if she lied. *Id.* at 52, 54. He then forced her to the car and got in the passenger's seat while she got into the driver's seat. *Id.* at 55. Ms. Hawkins-Ross testified that the man took her black Anne Klein purse, which contained \$60, her driver's license, Smart Trip cards, Social Security card, a Bank of America card, and a Navy Federal Credit Union card. *Id.* at 55-56, 58. He also took her second, personal cell phone—a Sprint Samsung Galaxy S3—and her cell phone chargers. *Id.* at 57-58. Ms. Hawkins-Ross testified that the man forced her to drive to the alley behind the apartment. *Id.* at 58. As he looked through her stuff, she jumped out of the car, grabbed her purse and keys, and ran. *Id.* at 59. She slipped through a fence, ran through a wooded area, and crossed the street to the Benco shopping center. *Id.* at 59-60. While running, she dropped her purse and keys. *Id.* at 65. She testified that she heard the man chasing her and yelling, "I'm really going to kill you now, bitch." *Id.* at 60.

When Ms. Hawkins-Ross got to the shopping center, she borrowed a cell phone and called 911. *Id.* at 61. She reported a robbery but said nothing of sexual assault to the operator. *Id.* at 64. Officer Justin Roth responded and was soon joined by Detective Douglas Carlson, Detective Griffin, and Detective Pulliam of the sexual assault unit. 10/30/14 at 160-161; 11/3/14 at 136-37. Ms. Hawkins-Ross testified that when she returned to the scene with the officers, she felt mucus in her throat and spit it out. 11/3/14 at 66. Detective Carlson advised the crime scene technician to collect the spit for evidence. *Id.* at 140. Ms. Hawkins-Ross was subsequently examined by a SANE at Washington Hospital Center. 11/3/14 at 10, 16.

On cross-examination, defense counsel called into question Ms. Hawkins-Ross's

credibility by impeaching her with a prior conviction for felony theft for withdrawing \$17,000 using a fraudulent identification card. *Id.* at 99. He exposed her bias by eliciting that she had misused her crime victim compensation for relocation by fraudulently cashing a government check made out to her new landlord. *Id.* at 95, 121-22. Defense counsel further cast doubt on Ms. Hawkins-Ross's account by eliciting that she knew she might have sex with her client and had a non-negotiable condom policy, but did not bring condoms. *Id.* at 110. Defense counsel suggested it was suspect that she did not initially report sexual assault when she called 911 or take the medications prescribed by the SANE. *Id.* at 119-20. Additionally, defense counsel emphasized that her DNA was not found on Mr. Jones's knife, even though she claimed the man had a knife to her neck throughout the incident. 11/4/14 at 317-19; 11/5/14 at 642-43.

C. Physical Evidence, Forensic Evidence, and Statements

Virtually all of the evidence connecting Mr. Jones to the alleged sexual assaults and robberies was recovered as a fruit of the government's warrantless use of the cell site simulator to locate Mr. Jones's phone. Officer Overmyer testified that he stopped Mr. Jones in the 4000 block of Minnesota Avenue, NE, on the morning of October 11, 2013. 11/3/14 at 174. He observed a black and silver knife, removed it from Mr. Jones, took it into custody, and placed Mr. Jones in handcuffs. *Id.* at 176, 196. When Detective Griffin arrived on the scene, he asked Mr. Jones where he lived, to which Mr. Jones responded, "566 Wilson Bridge Road . . . in Oxon Hill, Maryland"—the address of Ms. Hawkins-Ross. *Id.* at 188-89.

Detective Griffin also spoke to Nora Williams, the passenger in the car, and recovered four cell phones from her purse—(1) a white iPhone; (2) a Samsung Galaxy phone; (3) another Samsung Galaxy phone; and (4) the black iPhone Ms. Williams had been using. *Id.* at 199, 201-03. From the car, the police recovered a black Sprint flip phone and a black Cricket phone. *Id.*

at 195, 206, 207. They also recovered a green and pink bag, two Smart Trip cards, and a cell phone charger. *Id.* at 210, 212-14. The car was registered to Prince Jones. *Id.* at 215.

Ms. Hancock identified her white iPhone, 10/29/14 at 397; Ms. Shipp identified her green and pink purse and HTC phone, 10/30/14 at 70-71; and Ms. Hawkins-Ross identified her Verizon flip phone, her Samsung phone, her phone charger, and her pink and black cell phone case, 11/3/14 at 74-76, 79, 81-83. Ms. Hawkins-Ross testified that her Smart Trip cards were unregistered and last used at National Airport, which was consistent with the records of the recovered cards. 11/3/15 at 85-86; 11/5/14 at 490-91. Ms. Williams identified her Galaxy Samsung phone. 11/4/14 at 363. She testified that Mr. Jones had a cracked Cricket phone in October 2013 and was switching to an iPhone. 11/4/14 at 366-67, 371. She testified that the recovered black iPhone had a picture of Mr. Jones's daughter and contained his mother's phone number. *Id.* at 373. Ms. Williams's phone numbers were under the entry "Lovee." *Id.* at 375.

In order to further prove that the black iPhone belonged to Prince Jones and connect it to the sexual assaults, Detective Pulliam testified about data extracted from the recovered phones and their call logs. *Id.* at 252-53. Detective Pulliam testified that the iPhone was associated with the number 240-313-5281 and the email accounts PEEJones22@gmail.com and PEJ724@gmail.com. *Id.* at 254. The web history on the phone revealed numerous visits to Backpage.com, including visits to Ms. Shipp's and Ms. Hawkins-Ross's advertisements. *Id.* at 255-59. One text message from the phone said, "Hey, dis Prince." *Id.* at 259. There were also several messages about selling a white iPhone. *Id.* at 259-62. There were similar messages on Ms. Williams's phone. *Id.* at 262, 269-70. The Cricket phone had the same email accounts as the black iPhone—PEEJones22@gmail.com and PEJ724@gmail.com—and thirty out of fifty contacts matched the black iPhone's contacts. *Id.* at 264. The Cricket phone also had multiple

visits to Backpage.com. *Id.* at 266. An extraction report from Ms. Shipp's phone showed that the 240-313-5281 number associated with the black iPhone had texted the address 4452 B Street, SE on October 9, 2013. *Id.* at 267. Call logs revealed back and forth calls between the black iPhone and Ms. Shipp's phone shortly after midnight on October 9, 2013. *Id.* at 273-75. There were also back and forth texts and calls between the iPhone and Ms. Hawkins-Ross's phone in the early hours of October 11, 2013. *Id.* at 275-76. Additionally, Shawn Jones, Mr. Jones's sister, testified that Mr. Jones's number was 240-313-5281 in October 2013. *Id.* at 347-48.

Luis DeJesus, an expert in the analysis of call detail and historical cell site records, examined the records for the 240-313-5281 number and the complainants' phones. 11/5/14 at 502-04. These records showed what towers the phones contacted to make calls. *Id.* at 503-07. He testified that twelve hours after the first incident, Ms. Shipp's phone, Ms. Hancock's phone, and the 240-313-5281 phone were used in close proximity. *Id.* at 525-28. Each phone made calls near 1679 Fort Davis Street, SE, *id.* at 528-29, which Ms. Jones identified as the address of Mr. Jones's mother, 11/4/14 at 341. Likewise, shortly after the incident with Ms. Hawkins-Ross, her phone and the 240-313-5281 phone were used in close proximity. 11/5/14 at 535.

Finally, the government presented a photograph of Mr. Jones's groin and DNA evidence. After arresting Mr. Jones, the police took a photograph of his shaved groin area. *Id.* at 221-22. The police also took a buccal swab to develop Mr. Jones's DNA profile. 11/5/14 at 495-96. Emily Head, a forensic biologist, compared a swab of the biological material that Ms. Hawkins-Ross spit into the grass to the DNA profiles of Ms. Hawkins-Ross and Mr. Jones. 11/4/14 at 283, 310, 324, 327. The sperm fraction matched the profile obtained from Mr. Jones's buccal swab and the non-sperm fraction matched Ms. Hawkins-Ross's DNA profile. *Id.* at 324, 327. No DNA was found on the knife. *Id.* at 318-19.

#### D. Identification Procedures

None of the complainants identified Mr. Jones in court. However, after Mr. Jones was arrested, each was shown a sequential photo array which included Mr. Jones. Ms. Shipp initially said, “[N]one of these are him.” 10/29/14 at 376. She then selected someone *other* than Mr. Jones, and said, “[T]his one looks more like him than the rest.” *Id.* Ms. Hancock said, “I’m not sure,” and did not pick out a particular person. *Id.* at 382. When Ms. Hawkins-Ross viewed the photograph of Mr. Jones, she said, “[I]t kind of looks like him.” 11/3/14 at 155-56. Unlike the other photo arrays, Ms. Hawkins-Ross’s photo array was not double-blind because Detective Carlson, who administered it, knew who the suspect was. *Id.* at 152, 165.

#### E. Testimony of Nora Williams

Ms. Williams testified that in October 2013, she was living with her grandfather at 626 Nova Avenue in Capitol Heights and training to become a nursing assistant on Minnesota Avenue. 11/4/14 at 377-78. On Wednesday, October 9, 2013, Mr. Jones drove her to her internship. *Id.* at 380. She testified that when she got in the car, she noticed a white iPhone in the back. *Id.* at 383-84. She tried to use it but it was locked. *Id.* at 386. She handed it to Mr. Jones and when he returned it, it was unlocked. *Id.* at 388. She testified that the email on the phone was associated with Christina Hancock, a name she did not recognize. *Id.* at 390. She rebooted the phone to factory reset and told Mr. Jones that she was going to sell it. *Id.* at 393. She then texted someone at Best Buy about selling the phone. *Id.* Ms. Williams acknowledged that it was her idea to sell the phone, not Mr. Jones’s. *Id.* at 446-47.

Ms. Williams testified that she spent all day on October 10, 2013 with Mr. Jones and was with him in his car having sex in front of her grandfather’s house from 11:00 p.m. to 1:00 a.m. the following morning. *Id.* at 395-396. She then went inside to take a shower while Mr. Jones

waited for her. *Id.* at 396-97. Ms. Williams testified that after her shower, she called Mr. Jones but he did not answer. *Id.* at 398. Shortly after, he called her back and said he had been asleep. *Id.* at 398-400. Ms. Williams did not check whether his car was in front of the house when she called him. *Id.* at 400. Ms. Williams testified that when she went back out to his car, she noticed a pink striped bag. *Id.* at 401. She looked through the bag and saw two Smart Trip cards, a Bank of America bank card, a Navy Federal bank card, and a piece of paper with numbers on it, which she assumed were personal identification numbers (“PINs”). *Id.* at 402-04. There was also a black Samsung Galaxy phone and a black flip phone. *Id.* at 403-404. The Galaxy phone was the same as hers, and she switched its pink and black case for her case. *Id.* at 404, 407. She put the Smart Trip cards on the side of the passenger door. *Id.* at 405.

Ms. Williams testified that she then asked Mr. Jones to take her to a Navy Federal ATM to withdraw money. *Id.* at 408. After a failed attempt, they stopped briefly at Wawa,<sup>10</sup> and then headed to a Bank of America ATM. *Id.* at 409-410. She tried various PINs while Mr. Jones waited in the car. *Id.* at 411, 413. One of them worked and Ms. Williams withdrew over \$100. *Id.* at 410-11. The government admitted a video of Ms. Williams rejoicing as she withdrew money. *Id.* at 412, 413. Ms. Williams testified that she asked Mr. Jones to hold the money for her, and he took her home to get some sleep. *Id.* at 414. The next morning, Mr. Jones picked up Ms. Williams to take her to her internship. *Id.* at 415. As they sat in the car in front of her internship site eating food from Wendy’s, the police approached the car. *Id.* at 415-16.<sup>11</sup>

---

<sup>10</sup> The parties stipulated that Ms. Hawkins-Ross’s Bank of America card was used to purchase goods at a Wawa in Capitol Heights, MD at 5:30 a.m. on October 11, 2013. 11/5/14 at 492.

<sup>11</sup> Shawn Jones, Mr. Jones’s sister, testified that Mr. Jones used to live with Porsha Taylor on B Street, 11/4/14 at 345, and the parties stipulated that Ms. Taylor lived at 4452 B Street, SE, apartment 102, in 2005 and 2006. 11/5/14 at 490.

## ARGUMENT

### **I. THE GOVERNMENT’S WARRANTLESS USE OF A CELL SITE SIMULATOR TO TRACK THE PRECISE LOCATION OF MR. JONES’S CELL PHONE WAS AN ILLEGAL SEARCH IN VIOLATION OF THE FOURTH AMENDMENT.**

Without getting a warrant, the government used proprietary law enforcement technology, known as a cell site simulator, to pinpoint the precise location of Mr. Jones’s phone. By masquerading as an AT&T cell tower and simulating its signals, the cell site simulator forced Mr. Jones’s phone to disconnect from the AT&T network and communicate with it instead. As a result, Mr. Jones’s cell phone was disabled. His phone dropped a call mid-conversation, and he was unable to make or receive additional calls despite seven attempts to do so. By “grab[bing]” Mr. Jones’s phone and “tak[ing] the phone’s transmissions,” the cell site simulator determined his phone’s precise distance and direction. 10/17/14 at 44, 99. The cell site simulator led the police to Mr. Jones’s parked red Saturn in the 4000 block of Minnesota Avenue, NE, where they recovered the bulk of the evidence used against him at trial.

Whether governmental use of a cell site simulator, commonly known as a stingray or IMSI catcher<sup>12</sup>, to track the location of a cell phone constitutes a Fourth Amendment search requiring a warrant is a question of first impression in this jurisdiction. Indeed, Mr. Jones is not aware of any appellate court that has ruled on this issue.<sup>13</sup> In large part, this is because until

---

<sup>12</sup> “StingRay” is the name of a line of cell site simulator technology manufactured and sold by the Harris Corporation to local, state, and federal law enforcement agencies. See Stephanie K. Pell & 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.L. & Tech. 1, 14-15 (Fall 2014) (hereinafter *Your Secret Stingray’s No Secret Anymore*). Asserting law enforcement privilege, the government declined to disclose the model of cell site simulator used in locating Mr. Jones. 10/17/14 at 67; R. 48.

<sup>13</sup> The only appellate decision that discusses cell site simulators is *State v. Tate*, 849 N.W.2d 798 (Wis. 2014), in which the government conceded that a search occurred, and the court simply “assume[d], without deciding, that tracking a cell phone using cell site information and a stingray constitutes a search that has constitutional implications.” *Id.* at 807. An appeal challenging the

recently, cell site simulators were kept secret from the public and courts as law enforcement employing the technology were required to sign nondisclosure agreements. *See, e.g.*, Pell & Soghoian, *Your Secret Stingray's No Secret Anymore*, 28 Harv. J.L. & Tech. at 37-38; Matt Richell, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. Times (March 15, 2015); Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, Baltimore Sun (Nov. 17, 2014) (hereinafter *Judge Threatens Detective*). Thus, virtually all of the cell phone litigation in federal and state courts has focused on cell site location information (CSLI) collected by wireless carriers and provided to law enforcement. Cell site simulators present a unique set of concerns because they surreptitiously collect very precise information about a cell phone's location, are a direct government intrusion involving no third-party involvement, and function by disabling the user's cell phone.

The Fourth Amendment protects against unreasonable searches and seizures. *United States v. Jones*, 132 S. Ct. 945, 949 (2012). “[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.” *Katz v. United States*, 389 U.S. 347, 357 (1967). The warrantless use of a cell site simulator to track the location of Mr. Jones's cell phone was an illegal search for two distinct and independent reasons. First, it was a government trespass of a constitutionally protected “effect”—Mr. Jones's phone—for the purpose of obtaining information. *Jones*, 132 S. Ct. at 949; *Riley v. California*, 134 S. Ct. 2473, 2493 (2014). On this basis alone, this Court should hold that the government's use of a cell site simulator to disable Mr. Jones's phone and convert it

---

warrantless use of a cell site simulator is pending before the Maryland Special Court of Appeals. *See State v. Kerron Andrews*, Case No. 114149007 (Balt. City Cir. Ct. – Crim. 2015), *appeal docketed*, No. 1496 (Md. Ct. Spec. App. Sept. 3, 2015).



into a government tracking device was a search. Second, to the extent this Court disagrees that a trespass occurred, the government's use of a cell site simulator was a search because it violated Mr. Jones's reasonable expectations of privacy. *See Katz*, 389 U.S. at 360. Because the government failed to get a warrant and the inevitable discovery doctrine did not apply, the fruits of the search should have been suppressed, and Mr. Jones's convictions must be reversed.

A. THE USE OF A CELL SITE SIMULATOR ON MR. JONES'S PHONE CONSTITUTED A TRESPASS UNDER *JONES V. UNITED STATES*.

The government committed a trespassory search, in violation of Mr. Jones's Fourth Amendment rights, when it used a cell site simulator to force his phone to disconnect from the AT&T network, communicate with the cell site simulator, and reveal its location. In *United States v. Jones*, 132 S. Ct. 945 (2012), the Supreme Court held that the warrantless placement of a GPS tracking device on an individual's vehicle to monitor the vehicle's movement on public streets constituted a search under the Fourth Amendment because it was a government trespass for the purpose of obtaining information. 132 S. Ct. at 949. Placing a GPS device on the undercarriage of the appellant's Jeep without his consent was common law trespass to chattels. *Id.* at 949, 962. Because a vehicle is an "effect" within the meaning of the Fourth Amendment, *id.* at 949, the government's installation of this device "encroached on a protected area," *id.* at 952. By "trespassorily insert[ing] the information-gathering device," the government violated the appellant's Fourth Amendment rights. *Id.*

Significantly, the Supreme Court analyzed the appellant's claim under a property-based trespass theory rather than the reasonable expectation of privacy test set forth in *Katz v. United States*, 389 U.S. 347 (1967). The Court explained that the text of the Fourth Amendment, which protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," reflects a close connection to property. *Id.* at 949.

A search occurs where a government trespass of an enumerated item is “conjoined with” an “attempt to find something or to obtain information.” *Id.* at 951 n.5; *see also id.* at 953 & n.8. The Court emphasized that *Katz*, 389 U.S. 347, which held that a search occurs when the government invades an individual’s “reasonable expectation of privacy” notwithstanding the absence of trespass, did not repudiate the Fourth Amendment’s concern for trespass upon a protected area. *Id.* Rather, the Court explained that “the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.” *Id.* at 952 (emphasis in original). *See also Florida v. Jardines*, 133 S. Ct. 1409, 1414, 1417 (2013) (stating that the “traditional property-based understanding of the Fourth Amendment” provides a “simple baseline” that “keeps easy cases easy”). The *Jones* Court acknowledged that “[s]ituations involving merely the transmission of electronic signals *without trespass* would *remain* subject to *Katz* analysis,” *id.* at 953 (first emphasis added; second emphasis in original). However, where a “classic trespassory search” occurs, no further analysis is necessary. *Id.* at 954.

Here, the government’s use of a cell site simulator to obtain information about the precise location of Mr. Jones’s phone was a search under the “common law trespassory test” because the government gathered locational information by trespassing on Mr. Jones’s phone. Common law trespass to chattels may be committed by “intentionally . . . using or intermeddling with a chattel in the possession of another.” Restatement (Second) of Torts § 217(b) (1965); *see also Pearson v. Dodd*, 410 F.2d 701, 707 n.30 (D.C. Cir. 1969) (citing Restatement (Second) of Torts § 217 (1965)). One who commits a trespass to a chattel is subject to liability if, “(a) he dispossesses the other of the chattel, or (b) the chattel is impaired as to its condition, quality, or value, or (c) the possessor is deprived of the use of the chattel for a substantial time, or (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a

legally protected interest.” Restatement (Second) of Torts § 218 (1965). A leading treatise on torts describes trespass to chattels as “a little brother of conversion”; it provides a cause of action for interferences with the possession of personal property “not sufficiently important to be classed as conversion.” Prosser & Keeton, Torts § 14, at 85-86 (5th ed. 1984).<sup>14</sup>

Although the trespass at issue in *Jones* involved the physical touching of his vehicle, modern courts have held that common law trespass to chattels encompasses unauthorized electronic contact which interferes or threatens to interfere with a computer system’s functioning. For example, in *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996), a California appeals court held that the automated searching of a telephone carrier’s system for long distance authorization codes supported a cause of action for trespass to chattels because it “overburdened the [plaintiff’s] system, denying some subscribers access to phone[] lines.” 54 Cal. Rptr. 2d at 471. The court reasoned that the electronic signals were “sufficiently tangible to support a trespass cause of action.” *Id.* at 473 n.6. Subsequently, federal courts have held that sending bulk electronic mail (or “spam”) constitutes actionable trespass to chattels where it interferes with the functioning of computer equipment. *See, e.g., CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (stating that “[e]lectronic signals generated and sent by computer” are “sufficiently physically tangible to support a trespass cause of action”); *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 448, 452 (E.D. Va. 1998) (holding that the “transmission of electrical signals through a computer network is sufficiently ‘physical’ contact to constitute a trespass to property”).

---

<sup>14</sup> Conversion, in contrast, is “an intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel.” Restatement (Second) of Torts § 222A(1) (1965).

Likewise, federal courts have held that unauthorized robotic data collection from a company's publicly accessible website is actionable as trespass to chattels. *See, e.g., Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 438 (2d Cir. 2004) (affirming preliminary injunction on a trespass to chattels claim where the defendant's "search robots" performed automated queries of plaintiff's database, "deplete[d] the capacity available at a given time for authorized end-users," and posed "risks to the integrity of [plaintiff]'s systems due to potential congestion and overload problems"); *eBay, Inc. v. Bidder's Edge*, 100 F. Supp. 2d 1058, 1069-72 (N.D. Cal. 2000) (granting preliminary injunction on trespass to chattels claim against auction aggregation site because of threat to plaintiff's system from continued recursive searching). Although Mr. Jones is not aware of any court that has decided whether the use of a cell site simulator constitutes a trespass to chattels for Fourth Amendment purposes, in *State v. Tate*, a Wisconsin case in which the government conceded that the use of a cell site simulator is a search, one judge opined that the intrusion at issue was a trespass. 849 N.W.2d 798, 824 (Wis. 2014) (Abrahamson, C.J., dissenting). She reasoned that "[a]ny electronic signal entering the individual's phone and modifying it or triggering a response in any way, however slight, implicates a trespassory search." *Id.*

Here, the government's use of a cell site simulator to determine the location of Mr. Jones's phone constituted a trespass to chattels because it interfered with the functioning of his cell phone and rendered it non-operational for making calls.<sup>15</sup> A cell phone is an "effect" under

---

<sup>15</sup> Call detail records show that between 11:23 a.m. and 11:31 a.m. EST, the approximate time that the police used the cell site simulator, Mr. Jones's phone attempted seven calls and all seven failed. 10/29/14 at 239-40. Immediately prior to this series of failed calls, Mr. Jones's phone had a 14-minute call from 11:09 a.m. to 11:23 a.m. EST. *See id.* at 266. At 11:25, his phone sent a text message to the other participant in this prior call which said, "Our call dropped." *Id.* at 249. There were six attempts to call this number back, all of which failed. *Id.* at 240, 267. An attempted call to one additional number also failed. *See id.* As both the government and defense

the Fourth Amendment. *See Riley*, 134 S.Ct. at 2493 (warrant generally required before searching a cell phone, even when the phone is searched incident to arrest); *Tracey*, 152 So.3d 504 (cell phones are “effects” within the meaning of the Fourth Amendment). The cell site simulator trespassed on this protected effect by “grab[bing] [Mr. Jones’s phone] and “hold[ing] on to it,” thereby preventing it from communicating with the network’s tower and making calls. 10/17/14 at 44. The interference with Mr. Jones’s private property was far more serious than the interference in *Jones*. While placing a GPS on the undercarriage of the appellant’s car was a technical trespass because it was an unauthorized physical intrusion on the appellant’s vehicle, the GPS did not diminish the appellant’s use and enjoyment of his car. Indeed, as the concurrence observed, “the GPS did not interfere in any way with the operation of the vehicle, for if any such interference had been detected, the device might have been discovered. 132 S. Ct. at 958 (Alito, J., concurring). Here, in contrast, the government’s use of the cell site simulator disabled Mr. Jones’s phone and prevented him from placing calls.

Moreover, the government’s use of a cell site simulator was also a trespass because it “usurp[ed]” Mr. Jones’s property and “convert[ed]” it into a government tracking device. *Silverman v. United States*, 365 U.S. 505, 507, 511 (1961). “One of the main rights attaching to property is the right to exclude others,” and one “who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude.” *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (citing W. Blackstone, Commentaries, Book 2, ch. 1). The Supreme Court recognized these principles in *Silverman*, in which the government recorded conversations using a “spike mike” that “usurp[ed] part of the

---

witnesses testified, use of a cell site simulator prevents phones from communicating with the network tower and making calls. 10/17/14 at 43-44, 99, 103; 10/29/14 at 228-30.

petitioners' house or office—a heating system which was an integral part of the premises occupied by the petitioners, a usurpation that was effected without their knowledge . . . and consent.” *Silverman*, 365 U.S. at 506-11. The use of the spike mike was a Fourth Amendment search because it worked by “ma[king] contact with a heating duct serving the house occupied by the petitioners thus converting their entire heating system into a conductor of sound.” *Id.* Because the government obtained information by “usurp[ing]” the petitioner’s property, the Court held that its conduct amounted to a search even though the physical intrusion was no more than a fraction of an inch and irrespective of whether it was a technical trespass under local property law relating to party walls. *Id.* at 511-12. Here, as in *Silverman*, the government usurped Mr. Jones’s cell phone by converting it into a tracking device that pinpointed his location while simultaneously disabling his phone. This was a trespassory search in violation of Mr. Jones’s Fourth Amendment rights.

**B. THE USE OF A CELL SITE SIMULATOR VIOLATED REASONABLE EXPECTATIONS OF PRIVACY UNDER *KATZ V. UNITED STATES*.**

If this Court disagrees that the government’s use of a cell site simulator was a trespass of Mr. Jones’s phone, he is nonetheless entitled to relief because the government’s use of a cell site simulator to convert his cell phone into a government tracking device and determine its precise location violated his reasonable expectations of privacy under *Katz v. United States*, 389 U.S. 347 (1967). *See Jones*, 132 S. Ct. at 953-54 (explaining that where no trespass occurs, courts must engage in the *Katz* analysis). In *Katz*, the Supreme Court held that government wiretapping of a public phone booth was a search, notwithstanding the lack of trespass, because Mr. Katz “justifiably relied” upon the privacy of the telephone booth. *Katz*, 389 U.S. at 353. Subsequent Supreme Court cases have adopted and applied the test set forth in Justice Harlan’s concurrence:

“[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.” *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)). See also *Smith v. Maryland*, 442 U.S. 735, 740 (1979); *California v. Ciraolo*, 476 U.S. 207, 211 (1986). Here, Mr. Jones had both a subjective and objective expectation of privacy in the location information emanating from his phone. See *Ciraolo*, 476 U.S. at 211 (*Katz* posits a two-part inquiry).

First, Mr. Jones exhibited an actual, subjective expectation of privacy in his phone’s location: he secured a prepaid phone not connected to his name or address and turned off its GPS function. 10/17/14 at 17, 80. Mr. Jones chose not to share his location with his cell phone carrier or with any third-party cell phone applications—*e.g.*, Google Maps, Facebook, Yelp—which might seek to use this information to provide better service. Just as Mr. *Katz* demonstrated a subjective expectation of privacy in his phone conversation by shutting the door to the public phone booth and paying the toll, *Katz*, 389 U.S. at 352, Mr. Jones demonstrated a subjective expectation of privacy by not registering the phone and turning off the GPS. Given that Mr. Jones chose to preclude his wireless carrier and cell phone applications from knowing his precise whereabouts, he surely did not expect the government to override his expectation of privacy by surreptitiously tracking his phone with a cell site simulator.

Second, Mr. Jones had a legitimate expectation of privacy in the location of his cell phone, and by extension, his location. A reasonable person would not expect that the government could, at any moment in time and without a warrant, determine his precise location by converting his personal cell phone into a government tracking device. Cell phones are an indispensable part of modern life. They are not merely communication devices but “cameras, video players, rolodexes, calendars, tape recorders, libraries, video players, diaries, albums,

televisions, maps, [and] newspapers.” *Riley*, 134 S. Ct. at 2489. As the Supreme Court recently observed, they “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 human anatomy.” *Id.* at 2484. Given their centrality, it is not surprising that people tend to have their phones on them at all times. According to one poll, “nearly three-quarters of smart phone 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 (citation omitted). Cell phones follow people as they perform the most intimate aspects of their lives. They thus “blur the historical distinction between public and private areas because cell phones emit signals from both places.” *State v. Earls*, 70 A.3d 630, 642 (N.J. 2013); *Commonwealth v. Augustine*, 4 N.E.3d 846, 864 (Mass. 2014). Cell site simulators intrude upon reasonable expectations of privacy because they can determine a cell phone’s precise location at virtually any moment, irrespective of the user’s actions. So long as the phone is powered on, a cell site simulator can capture its signals and pinpoint its location.<sup>16</sup>

As the New Jersey Supreme Court sagely observed in the context of CSLI obtained from service providers, people buy cell phones to function in the daily world and reasonably do not expect the police to convert their personal cell phones into government tracking devices that can locate them at any given point in time:

[C]ell phones are not meant to serve as tracking devices to locate their owners wherever they may be. People buy cell phones to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a cell phone to share detailed information about their whereabouts with the police . . . Citizens have a legitimate privacy interest in such information. Although individuals may be generally aware that their phones can be tracked, most people do not realize the extent of modern tracking capabilities and reasonably do not expect law enforcement to convert their phones into

---

<sup>16</sup> It is unreasonable to expect a person to turn off his phone “just to assure privacy from governmental intrusion.” *Tracey*, 152 So. 3d at 523. Such a requirement “places an unreasonable burden on the user to forego necessary use of [a] cell phone, a device now considered essential by much of the populace.” *Id.*



precise, possibly continuous tracking tools.

*Earls*, 70 A.3d at 643.

The New Jersey court's additional observation that people are unaware of the extent of modern tracking capabilities is particularly apt in the context of cell site simulators, which the government purposefully kept secret from the public, and in some cases the courts, for years. Indeed, recent reports suggest that although cell site simulators have been in use for over twenty years, they largely escaped public and judicial scrutiny because the government took steps to prevent disclosure. This was accomplished through a "purposeful lack of disclosure to magistrate judges when seeking approval to use a cell site simulator in a criminal investigation, strict nondisclosure agreements with state and local law enforcement, and essentially across-the-board refusals to turn over documents relating to cell site simulators in response to Freedom of Information Act . . . and public records requests." Pell & Soghoian, *Your Secret Stingray's No Secret Anymore*, 28 Harv. J.L. & Tech. at 35-37 (citing cases where authorities had not been candid with magistrate judges about the technology used or declined to seek a warrant because they did not want to reveal information about cell site simulators). Last year, *The New York Times* reported that police departments are required to sign strict nondisclosure agreements preventing them from saying almost anything about the technology. Matt Richell, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. Times (Mar. 15, 2015); *See also* Fenton, *Judge Threatens Detective*, Baltimore Sun (Nov. 14, 2014) (officer refused to testify as to how he ascertained a phone's location, citing nondisclosure agreement).

In response to recent press about the warrantless use of cell site simulators, lawmakers have called for reform,<sup>17</sup> and the Department of Justice ("DOJ") and Department of Homeland

---

<sup>17</sup> On December 23, 2014, Senator Patrick Leahy, Chairman of the Senate Judiciary Committee, and Charles Grassley, the Ranking Member, sent a letter to the Attorney General and Secretary

Security (“DHS”) have responded by adopting a warrant policy. *See* DOJ Policy Guidance: Cell Site Simulator Technology, Sept. 3, 2015; DHS Policy Directive 047-02, Oct. 19, 2015. The political outcry to the warrantless use of cell site simulators and the response by federal agencies to implement a warrant requirement are strong indicia that society deems reasonable the expectation that the government will not use a cell site simulator to track a person’s location.

Although Mr. Jones is not aware of any appellate court cases analyzing the constitutionality of the warrantless use of a cell site simulator, several courts have held that cell phone users have a reasonable expectation of privacy in historical and real time CSLI<sup>18</sup> collected by their wireless carriers. In *Tracey*, the Florida Supreme Court held that “the use of [appellant’s] cell site location information emanating from his cell phone in order to track him in real time was a search within the purview of the Fourth Amendment for which probable cause was required.” 152 So. 3d at 526. Likewise, in *Earls*, the New Jersey Supreme Court analyzed the identically worded state analog to the Fourth Amendment and held that “police must obtain a warrant based on a showing of probable cause, or qualify for an exception to the warrant

---

of Homeland Security expressing concerns about the privacy implications of cell site simulators and seeking information about whether warrants are sought. Letter from Patrick Leahy and Charles Grassley, U.S. Senators, to Eric Holder, Att’y Gen., and Jeh Johnson, Sec’y of Homeland Security (Dec. 23, 2014) (on file with author), *available at* <http://www.grassley.senate.gov/sites/default/files/news/upload/2014-12-23%20PJL%20and%20CEG%20to%20DOJ%20and%20DHS%20%28cell-site%20simulators%29.pdf> (last visited Feb. 8, 2016).

On November 2, 2015, Representatives Jason Chaffetz, John Conyers, and Peter Welch introduced bipartisan legislation that would require federal and local law enforcement to get a warrant before using a cell site simulator. Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. Act (1st Sess. 2015).

<sup>18</sup> Historical CSLI refers to the past location of a cell phone derived from a cell phone company’s records kept in the ordinary course of business whereas real time CSLI is prospective location tracking by the cell phone companies for the purpose of police investigation. *See* R. Craig Curtis et al., *Using Technology the Founders Never Dreamed Of: Cell Phones as Tracking Devices and the Fourth Amendment*, 4 U. Denv. Crim. L. Rev. 61, 63 (2014).

requirement, to obtain tracking information through the use of a cell phone.” 70 A.3d at 644. *See also Augustine*, 4 N.E.3d at 866 (holding that government-compelled production of CSLI was a search under art. 14 of the state constitution, the state analog to the Fourth Amendment).

Those courts that have held that the government can obtain CSLI from cell phone carriers without a warrant have generally ruled on the basis of the third-party doctrine—that individuals have no reasonable expectation of privacy in business records owned and maintained by a third party. *See United States v. Davis*, 785 F.3d 498, 511 (11th Cir. 2015) (en banc) (holding that petitioner had “no subjective or objective reasonable expectation of privacy in [cell phone company]’s business records showing the cell tower locations that wirelessly connected his calls”); *In re Application of United States for Historical Cell Site Data*, 724 F.3d 600, 610-13 (5th Cir. 2013) (emphasizing that the telephone company, not the government, collected the CSLI in the first instance and for a variety of legitimate business interests); *State v. Perry*, 776 S.E.2d 528, 538, 542 (N.C. Ct. App. 2015) (holding that defendant had no reasonable expectation of privacy in the third-party records provided by AT&T).<sup>19</sup> The rationale of the third-party doctrine is that when an individual “voluntarily convey[s]” information to a third party for “legitimate business purposes,” he “assume[s] the risk that the information [will] be divulged to police.” *Smith v. Maryland*, 442 U.S. 735, 743-745 (1979). In contrast, courts

---

<sup>19</sup> The one federal appellate case that held there was no Fourth Amendment violation where the government obtained CSLI from a cell phone company on a ground other than the third-party doctrine—*United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012)—is flawed because it misapprehends Supreme Court precedent and is inapposite to cell site simulators. The court held that where the government uses CSLI to track an individual on public roads, *United States v. Knotts*, 460 U.S. 276 (1983) controls, and there is no expectation of privacy. *Skinner*, 690 F.3d at 777-78. However, unlike the beeper in *Knotts*, a cell site simulator does not merely “augment the sensory faculties bestowed upon [the officers] at birth” and enhance their visual surveillance of a suspect. 460 U.S. at 282. It is a wholly different means of locating a person without having any information other than his IMSI. Moreover, it implicates far greater privacy concerns than a beeper in a vehicle because of the cell site simulator’s precision and the reality that cell phones are almost always on one’s person and move fluidly between private and public spaces.

holding that a warrant is required to obtain CSLI from phone companies have rejected the notion that cell phone users, by virtue of having a cell phone, consent to third-party use of their location information for unrelated purposes, and have concluded that the third-party doctrine does not apply. *See, e.g., Tracey*, 152 So. 3d at 522; *Augustine*, 4 N.E.3d at 863; *Earls*, 70 A.3d at 641.<sup>20</sup>

Whatever the wisdom of applying the third-party doctrine to CSLI obtained from cell phone companies, the third-party doctrine most certainly does *not* apply to cell site simulators because there is *no third-party involvement*. Government use of a cell site simulator does not involve any third-party records or participation by cell phone carriers. Where, as here, the GPS function is turned off on a phone, cell phone companies do not collect information about the user's precise location in the ordinary course of business. To the contrary, Sergeant Perkins testified that AT&T could only provide information about what tower Mr. Jones's cell phone was communicating with—a much broader geographic area. Instead, the government used its own proprietary law enforcement technology to track the precise location of Mr. Jones's phone. This was a direct government intrusion that was not justified by any third-party interest or practice. Mr. Jones did not consent or reasonably expect the government to surreptitiously use secret law enforcement technology to ascertain his whereabouts at any moment in time.

C. CONTRARY TO THE TRIAL COURT'S RULING, THE INEVITABLE DISCOVERY DOCTRINE DOES NOT APPLY.

The trial judge declined to rule on whether the warrantless use of a cell site simulator to locate Mr. Jones's phone was a search under the Fourth Amendment. Rather, she ruled that

---

<sup>20</sup> Significantly, the Fifth Circuit limited its CSLI opinion to the narrow issue of "*historical* cell site information for specified cell phones at the points at which the user places and terminates a call," and left open the question of whether a warrant is required where, as here, "*the Government surreptitiously . . . hijacks the phone's GPS, with or without the service provider's help.*" *In re U.S. for Historical Cell Site Data*, 724 F.3d at 615 (second emphasis added).

assuming there was a search, it did not violate his Fourth Amendment rights under the inevitable discovery doctrine because “had [the police] switched over” to use the complainant’s phone number instead, “they would have gotten to the exact same place.” 10/29/14 at 310. The trial judge’s ruling was erroneous because she misapprehended the strict requirements of the inevitable discovery doctrine. Contrary to her ruling, the inevitable discovery doctrine did not apply for two independent reasons: (1) the police had not commenced using the cell site simulator on the complainant’s phone prior to the illegal search of Mr. Jones’s phone; and (2) the government did not meet its burden to show with certainty that the cell site simulator would have been successful at locating the complaint’s phone and yielded the same results.<sup>21</sup>

“The inevitable discovery doctrine provides that, even though the police have obtained evidence as a result of illegal conduct, the evidence still may be admitted ‘[i]f the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means.’” *Hicks v. United States*, 730 A.2d 657, 659 (D.C. 1999) (quoting *Nix v. Williams*, 467 U.S. 431, 444 (1984) (alteration in original)). As the doctrine’s name implies, the government must prove that discovery of the evidence was “truly inevitable,” not merely possible or even likely. *United States v. Allen*, 436 A.2d 1303, 1310 (D.C. 1981). “[O]nly if the court is persuaded ‘with certainty’ that the evidence would have been discovered lawfully may the exclusionary rule be waived.” *Id.* (citation omitted) (emphasis added); *United States v. Heath*, 455 F.3d 52, 58 (2d Cir. 2006) (“[T]he government cannot prevail under the inevitable discovery doctrine merely by establishing that it is more probable than not that the

---

<sup>21</sup> The trial court correctly found there were no exigent circumstances given the time lapse before the cell site simulator search and because one of the two MPD teams on the case could have gotten a warrant during that interval. 10/29/14 at 311. *See, e.g., Missouri v. McNeely*, 133 S. Ct. 1552, 1561-63 (2013) (“[W]here police officers can reasonably obtain a warrant . . . without . . . undermining the efficacy of the search, the Fourth Amendment mandates that they do so.”).

disputed evidence would have been obtained without the constitutional violation.”); 6 Wayne R. LaFare, *Search & Seizure* § 11.4(a), at 276 (4th ed. 2004) (“The significance of the word ‘would’ cannot be overemphasized. It is not enough to show that the evidence ‘might’ or ‘could’ have been otherwise obtained.”) (other internal quotation marks and citation omitted).

Critically, the inevitable discovery doctrine “involves *no speculative elements* but focuses [instead] on demonstrated historical facts capable of ready verification or impeachment.” *Hicks*, 730 A.2d at 659 (quoting *Williams*, 467 U.S. at 444-45 n.5) (emphasis added). Therefore, this Court has said that the inevitable discovery doctrine requires the government to prove two things. First, “the lawful process which would have ended in the inevitable discovery must have *commenced* before the constitutionally invalid [search or seizure].” *Id.* at 659 (emphasis added) (quotation omitted); *McFerguson v. United States*, 770 A.2d 66, 75 (D.C. 2001) (same); *Douglas-Bey v. United States*, 490 A.2d 1137, 1139 n.6 (D.C. 1985) (same). Second, “there must be ‘the requisite actuality’ that the discovery would have ultimately been made by lawful means.” *Hicks*, 730 A.2d at 659 (quoting *Hilliard v. United States*, 638 A.2d 698, 707 (D.C. 1994)); *McFerguson*, 770 A.2d at 75 (same). Here, the government did not meet its burden on either prong.

First, the government did not “commence” tracking the complainant’s cell phone with the cell site simulator “before” using it on Mr. Jones’s phone as required by the inevitable discovery doctrine. Sergeant Perkins testified that the police had only one working cell site simulator and he used it on *one* of the two phones. Although he did not remember which phone he used it on, in light of the evidence of Mr. Jones’s seven failed calls at the time of the cell site simulator, the trial court found that the government did not meet its burden to show that it had used the device on the complainant’s phone. 10/29/14 at 306. To prevail on inevitable discovery, however, the government was required to show that it had started tracking the complainant’s phone with the cell

site simulator before using a cell site simulator on Mr. Jones's phone and then continued to do so. Because the government tracked only one phone using a cell site simulator and the evidence suggests that it was Mr. Jones's phone, the inevitable discovery doctrine does not apply.

Second, the government did not adduce any evidence from which this Court can conclude "with certainty" that even if the government had commenced using the cell site simulator on the complainant's phone, which was an HTC phone on the Sprint network, the police would have successfully located Mr. Jones. The government presented no expert testimony about the functioning of the cell site simulator, choosing instead to present only lay testimony about how the field operators use the device to locate phones. The government likewise refused to acknowledge the manufacturer and model of the device that was employed in this case. Consequently, there is no evidence in the record about the failure rate of the cell site simulator or whether it statistically works better with certain models of phones or on certain networks. Likewise, because the technology is secret, the answers to these questions are most certainly beyond the ken of the trial court. On this record, the trial court simply did not know whether the failure rate of the cell site simulator used was 50% or 1%. Nor did it know whether it was better at simulating cell towers on the AT&T network versus the Sprint network, or at communicating with iPhones versus HTC phones. Given the dearth of information about the reliability of cell site simulators, it is "speculative," *Hicks*, 730 A.2d at 659, whether the government would have located Mr. Jones using Ms. Shipp's phone, and the inevitable discovery doctrine does not apply.

**D. THE FRUITS OF THE ILLEGAL SEARCH SHOULD HAVE BEEN SUPPRESSED.**

Because the police used a cell site simulator, in violation of the Fourth Amendment, the trial court should have suppressed the evidence obtained as a result of that search.<sup>22</sup> "Generally,

---

<sup>22</sup> The government's argument below that suppression is not the appropriate remedy because it is

when physical or testimonial evidence is uncovered by an illegal search or seizure, it must be suppressed as the ‘fruit of the poisonous tree.’” *Wilson v. United States*, 102 A.3d 751, 753 (D.C. 2014) (quotation omitted). *See also Wong Sun v. United States*, 371 U.S. 471, 484–86 (1963). The exclusionary rule not only excludes evidence that is the *primary* result of the violation, but “also prohibits the introduction of *derivative* evidence . . . that is the product of the primary evidence, or that is otherwise acquired as an indirect result of the unlawful search.” *Murray v. United States*, 487 U.S. 533, 536-37 (1988) (emphasis added) (citation omitted). “[T]he exclusionary rule applies unless the government proves that ‘the unlawful conduct has become so attenuated or has been interrupted by some intervening circumstances so as to remove the ‘taint’ imposed upon that evidence by the original illegality.’” *Gordon v. United States*, 120 A.3d 73, 85 (D.C. 2015) (quoting *United States v. Crews*, 445 U.S. 463, 471 (1980)). Here, the following categories of evidence should have been excluded:

1. Mr. Jones’s Knife and Statement to Police

As a direct result of the government’s cell site simulator, the police pinpointed Mr. Jones’s location in a red Saturn, seized him, frisked him, and asked for his identifying information. The flip knife on his person and his statement that he lived at 566 Wilson Bridge Road in Oxon Hill, Maryland—Ms. Hawkins-Ross’s address—were direct fruits of this illegal search and should have been suppressed. *Wong Sun*, 371 U.S. at 484-86.

2. Phones Recovered from Ms. Williams’s Purse

The phones recovered from Ms. Williams’s purse—Mr. Jones’s iPhone, Ms. Williams’s Samsung Galaxy phone, Ms. Hawkins-Ross’s Samsung Galaxy phone, and Ms. Hancock’s

---

not provided for in 18 U.S.C. § 3121(d), the pen register statute, *see* App’x C, misses the point. Mr. Jones did not raise a statutory claim, but a Fourth Amendment claim, where suppression is the standard remedy. *Wong Sun v. United States*, 371 U.S. 471, 484 (1963).



iPhone—should have been suppressed because Ms. Williams’s consent to search her purse was a “direct product[] of th[e] unlawful [cell site simulator search],” and there were “no intervening events of significance whatsoever.” *Allen*, 436 A.2d at 1309 (citation omitted) (holding that evidence seized from cab must be suppressed because defendant’s consent was a direct product of the unlawful detention). The Supreme Court’s seminal decision in *Wong Sun*, 371 U.S. 471, is on point. In that case, after Toy was illegally arrested, he responded to police questioning about the location of narcotics and provided the name and address of Johnny Yee. *Id.* at 474-75. The police went to Yee’s house, and Yee “surrendered” the narcotics to the police. *Id.* at 475. In assessing whether the narcotics must be suppressed as to Toy notwithstanding that Yee willingly gave them to the police, the Court explained that the “apt question” is “whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.” *Id.* at 488. The Court held that because the narcotics were “come at by exploitation of [the] illegality,” they could not be used against Toy. *Id.*

Subsequent to *Wong Sun*, the Supreme Court enumerated factors to guide courts in determining whether evidence was obtained through “means sufficiently distinguishable to be purged of the primary taint.” *Id.* In the context of physical evidence, these factors include: “the temporal proximity” of the illegality and evidence; “the presence of intervening circumstances”; and “the purpose and flagrancy of the official misconduct.” *Brown v. Illinois*, 422 U.S. 590, 604-05 (1975); *Gordon*, 120 A.3d at 85. Applying these factors, courts have held that consent to a search in the immediate aftermath of an illegal search or seizure is tainted. This applies to consent given by a third party as well as consent given by the defendant. For example, in *United States v. Maez*, the Tenth Circuit held that the wife’s consent to search the shared trailer home

was tainted by the illegal arrest of her husband, notwithstanding a signed consent form, because she gave consent thirty minutes after a SWAT team surrounded their home, summoned the occupants with a bull horn, and arrested her husband without a warrant. 872 F.2d 1444, 1447, 1455 (10th Cir. 1989). The court emphasized the proximity of the consent to the illegal arrest, the lack of intervening circumstances, and the frightening scenario. *Id.* at 1455. Likewise, in *United States v. Oaxaca*, the Ninth Circuit held that the sister's consent to a search of the defendant's bedroom was tainted by the illegal arrest of the defendant because it was given "mere moments after running to the garage, where she saw several armed DEA agents and her brother on his knees, already under arrest." 233 F.3d 1154, 1158 (9th Cir. 2000).<sup>23</sup>

Here, Ms. Williams's consent "was come at by exploitation of" the illegal cell site simulator search. First, and most importantly, the police asked for consent *immediately* after using the cell site simulator to locate Mr. Jones and arrest him. The police handcuffed Mr. Jones and then asked Ms. Williams to step into their police vehicle. The officers told her that Mr. Jones was going to be arrested and that they believed there was evidence of a crime in her purse. Although they asked for consent to search her purse, they told her they would seize her purse and get a warrant if she declined. After effectively being told that her purse would be searched either way, Ms. Williams signed a consent form. Second, there were no intervening events to dissipate the taint between the illegal cell site simulator search and Ms. Williams's consent. Third, the police misconduct was flagrant. Not only did they fail to get a warrant, they did not seek any type of court order during the three-to-four-hour period between the technical service unit coming on the case and using the cell site simulator. *Cf. Davis*, 785 F.3d at 505 (18 U.S.C. §

---

<sup>23</sup> See also *United States v. Washington*, 490 F.3d 765, 777 (9th Cir. 2007) (defendant's consent to search car did not purge taint of illegal seizure); *United States v. Gooding*, 695 F.2d 78, 84 (4th Cir. 1982) (same); *United States v. Miller*, 821 F.2d 546, 550 (11th Cir. 1987) (same).

2703(c) requires law enforcement, at a minimum, to “obtain a court order and present to a judge specific and articulable facts” before obtaining records from a service provider). As the trial court correctly observed, one of the two police units working the case could have sought a warrant during that time period. Accordingly, the recovered cell phones must be suppressed.

### 3. Evidence Recovered from Mr. Jones’s Car

The robbery proceeds recovered during the subsequent search of Mr. Jones’s car—Ms. Hawkins-Ross’s Verizon flip phone, Ms. Shipp’s HTC phone, Ms. Shipp’s purse, two Smart Trip cards, and a cell phone charger—must be suppressed as “derivative evidence” of the unlawful cell site simulator search. *Murray*, 487 U.S. at 536. Immediately after using the cell site simulator to locate Mr. Jones and arresting him, the police seized his car and applied for a search warrant. The affidavit in support of the warrant listed the fruits of the illegal search: the complainant’s phones, the knife, and Ms. Hawkins-Ross’s photo array identification. App’x H. The derivative evidence recovered during the car search is tainted for two independent reasons: (1) the officers’ “decision to seek the [search] warrant was prompted by” evidence obtained pursuant to the illegal cell site simulator search; and (2) “information obtained” from the illegal cell site simulator search was “presented to the [judge] and affected his decision to issue the warrant.” *Id.* at 542 (describing circumstances in which evidence obtained pursuant to a warrant is tainted and must be suppressed).

### 4. Extraction Reports from the Recovered Phones

Likewise, because the cell phones recovered from Mr. Jones’s car and Ms. Williams’s purse were tainted, the data extracted directly from these phones—*i.e.*, text messages, address books, web history, etc.— must also be suppressed as derivative evidence. As with the car search, the tainted evidence “prompted” the government to get a search warrant to extract data from the phones and was “presented to the [judge]” in the affidavit in support of the search

warrant. App'x I, J.<sup>24</sup>.

5. Ms. Williams's Testimony

Ms. Williams's testimony should have been suppressed in its entirety because it was "so closely" linked to the illegal cell site simulator search. *United States v. Rubalcava-Montoya*, 597 F.2d 140, 144 (9th Cir. 1979). In *United States v. Ceccolini*, 435 U.S. 268 (1978), the Supreme Court set forth factors for determining when the exclusionary rule should be invoked to exclude the testimony of a live witness: (1) whether the testimony was an act of free will in no way coerced or even induced by official authority as a result of the illegality, 435 U.S. at 278; (2) whether the evidence discovered as a result of the illegality was used in questioning the witness, *id.* at 279; (3) the time elapsed between the illegality and contact with the witness, *id.*; (4) whether the identity of the witness was already known to the police, *id.*; and (5) whether the illegality was made with the intention of discovering evidence, *id.* at 280.

Following *Ceccolini*, the D.C. Circuit held in *United States v. Scios* that a witness's testimony should have been suppressed where the police discovered his existence after illegally searching the defendant's files and the witness only testified after being threatened with contempt. 590 F.2d 956 (D.C. Cir. 1978) (en banc). The court emphasized the witness's initial refusal to consult with authorities; that he testified under threat of a contempt citation; that his existence was unknown to authorities prior to the illegal search; and that the purpose of the search was to "gain evidence" against the defendant. *Id.* at 963. Similarly, in *United States v. Ramirez-Sandoval*, the Ninth Circuit excluded witness testimony where a police officer illegally

---

<sup>24</sup> A motion to supplement the record with the warrants to search the recovered cell phones and Mr. Jones's car, and the affidavits in support of these warrants, has been filed with the Court. Mr. Jones only received the odd-numbered pages of the warrant to search Mr. Jones's car in discovery. However, defense counsel is working with the government to obtain the full document and will provide it to the court when she receives it.

searched the sun visor of a car, discovered papers with names and numbers, questioned the passengers about these papers, and elicited that the papers documented monetary sums paid to the defendant to be smuggled into the United States. 872 F.2d 1392, 1398 (9th Cir. 1989). Significant factors in the court's analysis were the temporal proximity of the illegal search and questioning; that the illegally discovered papers were used in questioning; that the identities of the undocumented immigrants were not previously known to the police; and that it was "not likely that these witnesses would have come forward of their own volition." *Id.* at 1397. *See also United States v. Ienco*, 182 F.3d 517, 530-31 (7th Cir. 1999) (witness testimony properly excluded where decision to testify in exchange for a lighter sentence was "dictated by [witness's] own precarious legal situation"; police disclosed recovered evidence during questioning; questioning occurred within hours of the illegality; and government did not demonstrate that witness's identity could have been discovered absent illegal arrests and searches); *Rubalcava-Montoya*, 597 F.2d at 144 (excluding testimony of undocumented immigrants found in truck because their testimony was "almost inextricably[] linked" with the illegal search).

Here, the *Ceccolini* factors weigh in favor of excluding Ms. Williams's testimony. First, and most critically, her testimony was not an act of free will. She testified that the police "forced" her to go with them for questioning and were "very intimidating." 11/4/14 at 421. Initially, she was not forthcoming and lied about where she got the phones. *Id.* at 420. At the Grand Jury, she asserted her Fifth Amendment right against self-incrimination. *Id.* at 424. She subsequently participated in a debriefing with the government but continued to lie, despite being told her statements could be used against her, because she was afraid of being locked up. *Id.* at 426-27. She did not finish the session. *Id.* at 427. Ms. Williams subsequently returned to the Grand Jury under subpoena but declined to keep speaking to the government. *Id.* at 427-28.

Ultimately, the government granted her immunity and she was compelled to testify by court order. *Id.* at 428-29. When asked how she felt about testifying at trial, she repeatedly said, “I don’t want to.” *Id.* at 432. As in *Scios*, Ms. Williams was not a willing witness.

Second, the subject of the questioning was evidence discovered as a result of the illegal search. The police wanted to know where Ms. Williams and Mr. Jones got the complainants’ phones, when she first saw Mr. Jones with the phones and other proceeds, and where Mr. Jones was at the time of the assaults. *See* 11/4/14 at 377-432. Third, Ms. Williams was questioned immediately after the illegality. After arresting Mr. Jones and discovering the phones in her purse, the police took her to the police station for questioning. Fourth, the government did not demonstrate that it would have discovered Ms. Williams in the absence of the illegality. Without the illegal search, it did not know the identity of the assailant, let alone Ms. Williams’s connection to Mr. Jones or to the phones. Moreover, Ms. Williams was not likely to come forward given her own precarious legal situation. Finally, the purpose of the cell site simulator was to identify the assailant and “gain evidence” to build a case against him. *Scios*, 590 F.2d at 963. Because of the “direct link” between the illegality and the procurement of Ms. Williams’s testimony, her testimony should have been excluded. *Ceccolini*, 435 U.S. at 278.

6. Ms. Hawkins-Ross’s Identification

Ms. Hawkins-Ross’s statement that the picture of Mr. Jones “kind of looks like him,” 11/3/14 at 155-56, must also be suppressed because the photo array was a direct product of the government’s illegal cell site simulator search. *See, e.g., Crews*, 445 U.S. at 477 (“pretrial identification obtained through use of the photograph taken during respondent’s illegal detention cannot be introduced”); *Bryant v. United States*, 599 A.2d 1107, 1113 (D.C. 1991) (suppressing show-up identification procedure where police acquired evidentiary basis for detaining the defendant as a result of the illegal search and seizure).

7. Mr. Jones's DNA Profile and Photograph of his Groin

Finally, Mr. Jones's DNA profile, obtained through a buccal swab, and the photograph of his groin must be suppressed because they were "acquired as an indirect result of the unlawful search." *Murray*, 487 U.S. at 537. The police took the photograph while Mr. Jones was in custody following the illegal cell site simulator search that led to his arrest. Therefore, it is a fruit of the illegality. *See, e.g., Hayes v. Florida*, 470 U.S. 811 (1985) (suppressing fingerprints taken at the police station as fruit of illegal detention). The buccal swab was similarly tainted. The court initially declined to issue an order for a DNA swab until after it determined probable cause. *See* 10/21/13 at 6, 117. The court ultimately found probable cause based in large part on tainted fruits—the stolen property and Mr. Jones's possession of a phone with the 240-313-5281 number. *Id.* at 115. As with the warrants for the car and cell phones, the "decision to seek the [court order] was prompted by" evidence obtained pursuant to the illegal cell site simulator search; and (2) "information obtained" from the illegal cell site simulator search was "presented to the [judge] and affected [the] decision to issue the [order]." 487 U.S. at 542.

E. THE TRIAL COURT'S ERROR IN FAILING TO SUPPRESS THE FRUITS OF THE ILLEGAL SEARCH WAS NOT HARMLESS.

The erroneous denial of Mr. Jones's suppression motion requires reversal unless the government can demonstrate that this constitutional error was "harmless beyond a reasonable doubt." *Chapman v. California*, 386 U.S. 18, 24 (1967). As this Court has admonished, the *Chapman* standard "is an exacting standard indeed." *Ellis v. United States*, 941 A.2d 1042, 1048 (D.C. 2008). "The properly admitted evidence against the defendant must be 'overwhelming,'" and "[t]he government must show that there is no 'reasonable possibility that the evidence complained of might have contributed to the conviction.'" *Id.* at 1049 (quoting *McCoy v. United States*, 890 A.2d 204, 212 (D.C. 2006); *Chapman*, 386 U.S. at 23). "[T]he 'inquiry [under

*Chapman*] . . . is not whether, in a trial that occurred without the error, a guilty verdict would surely have been rendered, but whether *the guilty verdict actually rendered in this trial was surely unattributable to the error.*” *Id.* (quoting *Sullivan v. Louisiana*, 508 U.S. 275, 279 (1993) (emphasis in *Ellis*)). The government cannot satisfy this heavy burden here.

The tainted fruits of the cell site simulator search constituted the vast majority of the government’s evidence. The physical evidence—an iPhone with the 240-313-5281 number that contacted Ms. Shipp and Ms. Hawkins-Ross; Ms. Hancock’s phone; Ms. Shipp’s phone; Ms. Hawkins-Ross’s two phones; Ms. Shipp’s pink and green bag; two Smart Trip cards; a cell phone charger; and a knife matching the description of the assailant’s knife—formed the heart of the government’s case. As the prosecutor told the jury, “Ladies and gentlemen, the evidence in this case is overwhelming. The defendant had so much stolen property on him.” 11/5/14 at 629. The prosecutor’s emphasis on these fruits in closing is “at least a highly relevant measure” of their prejudicial impact. *Andrews v. United States*, 922 A.2d 449, 461 (D.C. 2007) (quoting *Garris v. United States*, 390 F.2d 862, 866 (D.C. Cir. 1968)).

The prosecutor understood that the phone with the 240-313-5281 number, the complainant’s property, and the knife powerfully corroborated the complainants’ accounts of being sexually assaulted and robbed and directly connected Mr. Jones to the alleged crimes.

This Court has recognized the persuasive force of physical evidence:

“[T]here is a general mental tendency, when a corporal object is produced as proving something, to assume, on sight of the object, all else that is implied in the case about it. The sight of it seems to prove all the rest.”

*Burleson v. United States*, 306 A.2d 659, 662 (D.C. 1973) (quoting 7 Wigmore on Evidence § 2129 (3d ed. 1940)). Likewise, “it is an inference of ancient vintage for a jury to find a defendant guilty of a robbery when that defendant exclusively possesses recently stolen property without satisfactorily explaining why.” *Ingram v. United States*, 592 A.2d 992, 999 (D.C. 1991)



(internal quotation marks omitted).

In addition to being strong evidence of the robbery, the stolen property and knife also corroborated the complainant's account of being forced to perform oral sex at knifepoint. Evidence that Mr. Jones robbed the complainants boosted their credibility and made their account of sexual assault more probable. In the absence of the proceeds and knife, Mr. Jones's consent defense would have had more force, particularly given the lack of physical evidence of sexual assault, Ms. Shipp's refusal to do a SANE examination, and Ms. Hawkins-Ross's failure to report sexual assault to the 911 operator. A jury may well have had a reasonable doubt that Mr. Jones responded to advertisements for escort services and had consensual oral sex with women who routinely perform sexual services for money. The defense that these escorts subsequently fabricated the sexual assault and robbery, possibly over a dispute about money, would have been far more powerful. Additionally, the combination of the cell phone extraction reports, Mr. Jones's DNA profile, Ms. Hawkins-Ross's statement that his picture "kind of looks like him," the photograph of his shaved groin, and Ms. Williams's testimony all powerfully suggested that Mr. Jones owned the 240-313-5281 phone and was the assailant.<sup>25</sup>

The fruits of the illegal search dramatically altered the evidentiary landscape of the case. Given the sheer magnitude of the tainted evidence and its probative force, the government cannot meet its burden to "show that there is no reasonable possibility that the evidence complained of might have contributed to the conviction." *Ellis*, 941 A.2d at 1049 (quotation omitted).


### CONCLUSION


For the foregoing reasons, Mr. Jones respectfully asks that his convictions be reversed.


---

<sup>25</sup> If this evidence had been excluded, Mr. Jones may well have pursued an entirely different defense such as misidentification. Notably, none of the witnesses identified Mr. Jones in court. Ms. Hancock failed to identify Mr. Jones from a photo array, and Ms. Shipp picked a different man. Without the tainted evidence, very little linked Mr. Jones to the alleged offenses.

Respectfully submitted,

  
\_\_\_\_\_  
Samia Fam  
Bar No. 394 445

  
\_\_\_\_\_  
Jaelyn Frankfurt  
Bar No. 415 252

  
\_\_\_\_\_  
\*Stefanie Schneider  
Bar No. 979 816

PUBLIC DEFENDER SERVICE  
FOR THE DISTRICT OF COLUMBIA  
633 Indiana Avenue, NW  
Washington, DC 20004  
(202) 628-1200

\*Counsel for Oral Argument

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing brief has been served, by hand, upon Elizabeth Trosman, Chief, Appellate Division, Office of the United States Attorney, 555 Fourth Street, NW, Washington, DC 20530, this 16th day of February, 2016.

  
\_\_\_\_\_  
Stefanie Schneider