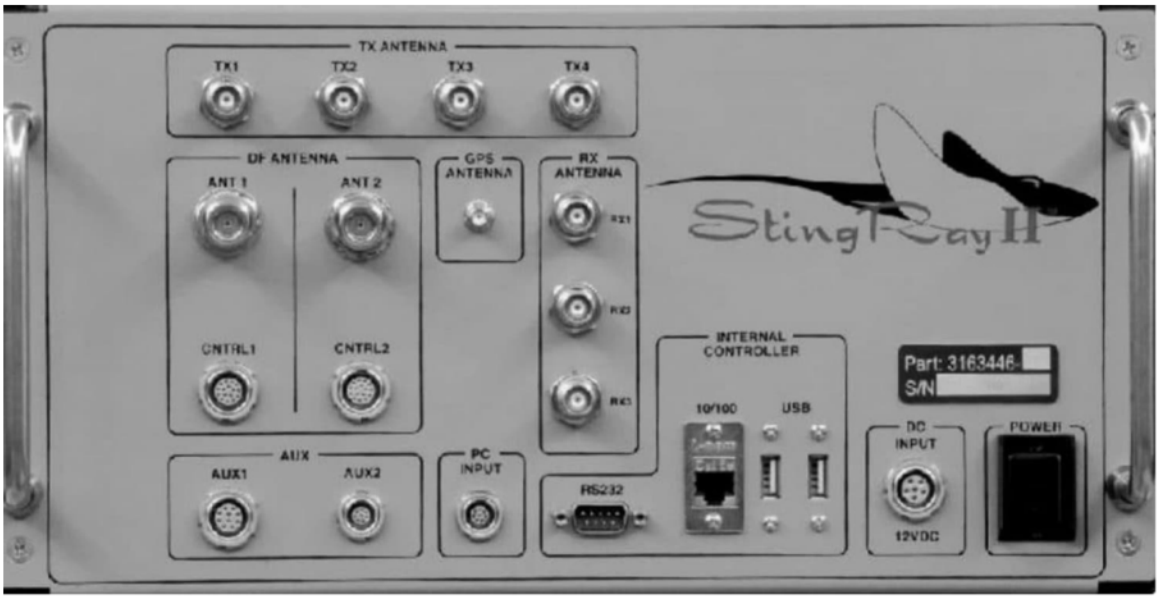

A "StingRay II," made by the Harris Corp., can redirect cellphone calls away from cell tower antennae and capture their identifying data and location. Police use them to find people. Some argue that that's an invasion of privacy. (Courtesy Harris Corp.)

A device that tricks cellphones into sending it their location information and has been used quietly by policeand federal agents for years, requires a search warrant before it is turned on, an appeals court in Washington ruled Thursday. It is the fourth such ruling by either a state appeals court or federal district court, and may end up deciding the issue unless the government takes the case to the U.S. Supreme Court or persuades the city's highest court to reverse the ruling.

The case against Prince Jones in 2013 involved D.C. police use of a "StingRay" cell-site simulator, which enables law enforcement to pinpoint the location of a cellphone more precisely than a phone company can when triangulating a signal between cell towers or using a phone's GPS function. Civil liberties advocates say the StingRay, by providing someone's location to police without court approval, is a violation of an individual's Fourth Amendment right not to be unreasonably searched. The D.C. Court of Appeals agreed in a 2 to 1 ruling, echoing similar rulings in the Maryland Court of Special Appeals and federal district courts in New York City and San Francisco.

"This opinion," said Nathan F. Wessler of the American Civil Liberties Union, who helped argue the case with the D.C. Public Defender Service, "joins the growing chorus of courts holding that the Fourth Amendment protects against warrantless use of invasive, covert technology to track people's phones. … We applaud today's opinion for erecting sensible and strong protections against the government violating people's privacy in the digital age."

The U.S. attorney's office in Washington declined to comment on the ruling. The prosecutors could ask for a rehearing by the three judge panel or the entire appeals court, and if those are denied take the case to the Supreme Court, though Wessler noted that the high court might not be inclined to take a case where there is no dispute among the lower court rulings.

The Justice Department issued policy guidance to its agencies in 2015 that a search warrant must be obtained for all StingRay uses, and though that is not binding on state and local police, the Metropolitan Police Department has said it would abide by that rule. The ACLU has counted 72 cell-site simulators in use in 24 states and the District, but believes there could be many more. Both D.C. and Baltimore police had signed an agreement with the FBI not to disclose or discuss their StingRay device publicly, court records show, and an FBI agent sat with prosecutors during Jones's trial to advise them on how to handle questions about the device.

The ruling by the D.C. Court of Appeals resulted in all the evidence in the case against Jones being thrown out, and a nine-count felony conviction for sexual abuse, kidnapping, armed robbery and threats being vacated.

Jones was arrested after he allegedly assaulted and robbed two women in separate incidents, after arranging to meet with them through Backpage.com for sexual liaisons. In both cases, the perpetrator took the victims' cellphones.

After the second incident, D.C. police compared the call records of the victims and found that the same phone number had been used to arrange both meetings. The police then obtained the mobile identification number for the man's phone, as well as the identification numbers for the victims' phones, and with the help of the phone companies obtained a general location for the phones, which police said appeared to be traveling together.

Once in the vicinity of the phones, the police turned on the StingRay, court records show, and punched in the identification number (different from the phone number) of the assailant's phone. The StingRay acts like a cell site antenna, and convinces cellphones to connect to it instead of a real cell site, providing the phone numbers and locations of the phones that connect. The phones are useless during this time because they aren't connected to an actual network, only the StingRay.

Before long, the assailant's prepaid cellphone was found on Jones, sitting in a parked car on Minnesota Avenue in Northeast Washington, as were the phones stolen from the victims, police said. The appeals court ruled, and the defense agreed, that if the police had used the StingRay on one of the victims' phones,

instead of Jones's phone, the search would have been legal because the victims consented to the search.

The judge in Jones's trial declined to suppress the phone seizure, which in turn led to the knife apparently used in the robberies, the discovery of the victims' phones and incriminating statements made by Jones and his girlfriend. But the ruling written by Associate Judge Corinne A. Beckwith, joined by Senior Judge Michael W. Farrell, threw out all of that evidence as "fruit of the poisonous tree," namely the StingRay.

"Locating and tracking a cell-site simulator," Beckwith wrote, "has the substantial potential to expose the owner's intimate personal information," particularly their movements and whereabouts. "A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will."

For that reason, Beckwith said, "the use of a cell-site simulator to locate Mr. Jones's phone invaded a reasonable expectation of privacy and was thus a search."

Prosecutors argued that everyone knows that the location of a cellphone can be tracked, and at oral argument one noted that every fleeing criminal on television dramas throws away or destroys their phone. Beckwith disregarded that approach, saying that "a person does not lose a reasonable expectation of privacy merely because he or she is made aware of the government's capacity to invade his or her privacy."

Associate Judge Phyllis D. Thompson dissented, though she wrote that under ordinary circumstances, she agreed that the government's use of a StingRay "likely violates the legitimate expectation of privacy." But Thompson said Jones forfeited that privacy when he drove around with the victims' stolen cellphones. Beckwith responded that Jones had not been charged or convicted of stealing the phones at the time of the search.

The StingRay issue is separate from another cellphone issue pending before the Supreme Court — whether law enforcement must obtain a warrant before obtaining a cellphone's historical location data from a phone company. Phone companies record which cell towers are used when a call is made, which police often use to demonstrate a person's whereabouts at the time of a crime. Those records can be obtained with a court order, and a lower standard of proof, rather than a warrant. The ACLU's Wessler said that Thursday's ruling was a "recognition that constitutional protections must keep pace with advancing technology, and is an important reminder of what is at stake as the Supreme

Court takes up the issue of police requests for historical cellphone location data."

From: (b)(6); (b)(7)(C)
Sent: 26 Sep 2016 15:18:42 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: Intro to Computers Networks and Cybercrime Presentation (updated as of 8.4.16).pptx
Attachments: Intro to Computers Networks and Cybercrime Presentation (updated as of 8.4.16).pptx

(b)(6); (b)(7)(C)

As discussed, please take a look at this PPT (updated through August). This is the training CLS has to give on Tuesday, October 4. I will plan to present with you watching, but if you feel comfortable with the material and want to present any of it, that works too!

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (b)(7)(C) Desk)
202-536- Cell)

From: (b)(6); (b)(7)(C)
Sent: 22 Nov 2017 19:57:34 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: Just FYSA; Article re: Cell Site Simulators

Tech Ops:

(b)(7)(E)

11/17 Article re: HSI use of Cell Site Simulators; just FYSA

Thanks, (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
(202) 732 (b)(6); (b)(7)(C) (office)
(202) 308 (cell)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 13 Jul 2016 20:51:55 +0000
To: (b)(6); (b)(7)(C)
Subject:
Attachments: US v Lambis.pdf

(b)(5)

Thanks (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Associate Legal Advisor
U.S. Immigration and Customs Enforcement
Office of the Principal Legal Advisor
Homeland Security Investigations Law Division
Criminal Law Section
(202) 732-(b)(6); (b)(7)(C) (office)
(202) 308- (iPhone)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Wednesday, July 13, 2016 3:20 PM
To: (b)(6); (b)(7)(C)
Subject: FW: Technical Question

(b)(6); (b)(7)(C)

Please see the message below from the FBI concerning authority to covertly record two party consent in states without a LE exception.

(b)(6); (b)(7)(C)
Section Chief
Title III Investigative Programs

Technical Operations Unit
ICE Homeland Security Investigations
U.S. Department of Homeland Security
703.551-6 (b)(6); (b)(7)(C) (Office)
571.238.1 (Cell)
(b)(6); (b)(7)(C)

With honor and integrity, we will safeguard the American people, our homeland, and our values.

From: (b)(6); (b)(7)(C)
Sent: Tuesday, June 07, 2016 3:34 PM
To: (b)(6); (b)(7)(C)
Subject: FW: Technical Question

From: (b)(6); (b)(7)(C)
Sent: Monday, June 06, 2016 2:17 PM
To: (b)(6); (b)(7)(C)
Subject: RE: Technical Question

(b)(7)(E); (b)(5)

From (b)(6); (b)(7)(C)
Sent: Monday, June 06, 2016 12:56 PM
To: (b)(6); (b)(7)(C)
Subject: RE: Technical Question

(b)(6);

What does OIA stand for?

Thanks,

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Wednesday, June 01, 2016 4:39 PM
To: (b)(6); (b)(7)(C)
Subject: RE: Technical Question

(b)(6); (b)(7)(C)

Sorry for my delay this morning. I am glad you had a nice weekend in NYC. I had a great time here in Oahu. I did some hiking and of course some shopping!

I thought the best way to answer your question was to provide the attached chart. I made some notations on it as well to clarify a few things. Please take a look and let me know if it is helpful or if you have any further questions.

(b)(6);
(b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Wednesday, June 01, 2016 6:36 AM
To: (b)(6); (b)(7)(C)
Subject: Technical Question

(b)(6); (b)(7)(C)

I hope you had a good holiday weekend. I was sad to have to return to work after a nice weekend in NYC.

(b)(7)(E); (b)(5)

Thanks,

(b)(6);
(b)(7)(C)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	
-against-	15cr734
RAYMOND LAMBIS,	OPINION & ORDER
Defendant.	

WILLIAM H. PAULEY III, District Judge:

Raymond Lambis moves to suppress narcotics and drug paraphernalia recovered by law enforcement agents in connection with a search of his apartment. Lambis's motion to suppress is granted.

BACKGROUND

In 2015, the Drug Enforcement Administration (the "DEA") conducted an investigation into an international drug-trafficking organization. As a part of that investigation, the DEA sought a warrant for pen register information and cell site location information ("CSLI") for a target cell phone. Pen register information is a record from the service provider of the telephone numbers dialed from a specific phone. CSLI is a record of non-content-based location information from the service provider derived from "pings" sent to cell sites by a target cell phone. CSLI allows the target phone's location to be approximated by providing a record of where the phone has been used.

Using CSLI, DEA agents were able to determine that the target cell phone was located in the general vicinity of "the Washington Heights area by 177th and Broadway." (April 12, 2016 Suppression Hearing Transcript ("Supp. Tr."), at 39.) However, this CSLI was not precise enough to identify "the specific apartment building," much less the specific unit in the

apartment complexes in the area. (Supp. Tr. at 39.)

To isolate the location more precisely, the DEA deployed a technician with a cell-site simulator to the intersection of 177th Street and Broadway. A cell-site simulator—sometimes referred to as a "StingRay," "Hailstorm," or "TriggerFish"—is a device that locates cell phones by mimicking the service provider's cell tower (or "cell site") and forcing cell phones to transmit "pings" to the simulator. The device then calculates the strength of the "pings" until the target phone is pinpointed. (See Supp. Tr. at 40.) Activating the cell-site simulator, the DEA technician first identified the apartment building with the strongest ping. Then, the technician entered that apartment building and walked the halls until he located the specific apartment where the signal was strongest. (Supp. Tr. at 41.)

The cell-site simulator identified Lambis's apartment as the most likely location of the target cell phone. That same evening, DEA agents knocked on Lambis's apartment door and obtained consent from Lambis's father to enter the apartment. (Supp. Tr. at 8–9.) Once in the apartment, DEA agents obtained Lambis's consent to search his bedroom. (Supp. Tr. at 13.) Ultimately, the agents recovered narcotics, three digital scales, empty zip lock bags, and other drug paraphernalia. (Supp. Tr. at 14.) Lambis seeks to suppress this evidence.

DISCUSSION

I. Fourth Amendment Search

The Fourth Amendment guarantees that all people shall be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. "[T]he underlying command of the Fourth Amendment is always that searches and seizures be reasonable." New Jersey v. T.L.O., 469 U.S. 325, 337 (1985). "[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). Barring a few narrow exceptions, "warrantless searches 'are per se unreasonable under the Fourth Amendment.'" City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (quoting Katz v. United States, 389 U.S. 347, 357 (1967)). The home has special significance under the Fourth Amendment. "'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" Kyllo, 533 U.S. at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

In Kyllo, the Supreme Court held that a Fourth Amendment search occurred when Government agents used a thermal-imaging device to detect infrared radiation emanating from a home. 533 U.S. at 40. In so holding, the Court rejected the Government's argument that because the device only detected "heat radiating from the external surface of the house," there was no "search." Kyllo, 533 U.S. at 35. The Court reasoned that distinguishing between "off-the-wall" observations and "through-the-wall surveillance" would "leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home." Kyllo, 533 U.S. at 35–36. Thus, the Court held that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." Kyllo, 533 U.S. at 40.

Here, as in Kyllo, the DEA's use of the cell-site simulator to locate Lambis's apartment was an unreasonable search because the "pings" from Lambis's cell phone to the nearest cell site were not readily available "to anyone who wanted to look" without the use of a cell-site simulator. See United States v. Knotts, 460 U.S. 276, 281 (1983); see also State v. Andrews, 227 Md. App. 350, *23 (Md. Ct. Spec. App. 2016) (holding that the use of a cell site

simulator requires a search warrant based on probable cause, and finding that the trial court properly suppressed evidence obtained through the use of the cell-site simulator). The DEA's use of the cell-site simulator revealed "details of the home that would previously have been unknowable without physical intrusion," Kyllo, 533 U.S. at 40, namely, that the target cell phone was located within Lambis's apartment. Moreover, the cell-site simulator is not a device "in general public use." Kyllo, 533 U.S. at 40. In fact, the DEA agent who testified at the hearing had never used one.

The Government counters that Kyllo is not implicated here. In Kyllo, the Court expressed concern that the Government could employ devices, like a thermal imaging device, to learn more intimate details about the interior of the home, such as "at what hour each night the lady of the house takes her daily sauna and bath." Kyllo, 533 U.S. at 38. The Government contends that because the only information to be gleaned from a cell-site simulator is the location of the target phone (for which the Government had already obtained a warrant for CSLI), no intimate details of the apartment would be revealed and Lambis's expectation of privacy would not be implicated. But the Second Circuit has rejected a similar argument even when the search at issue could "disclose only the presence or absence of narcotics" in a person's home. United States v. Thomas, 757 F.2d 1359, 1366–67 (2d Cir. 1985) (holding that a canine sniff that "constitutes a search under the Fourth Amendment . . . when employed at a person's home").

The Government attempts to diminish the power of Second Circuit precedent by noting that Thomas represents a minority position among circuit courts. But this Court need not be mired in the Serbonian Bog of circuit splits. An electronic search for a cell phone inside an apartment is far more intrusive than a canine sniff because, unlike narcotics, cell phones are neither contraband nor illegal. In fact, they are ubiquitous. Because the vast majority of the

population uses cell phones lawfully on a daily basis, "one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful." Kyllo, 533 U.S. at 38; see also United States v. Jacobsen, 466 U.S. 109, 124 (1984) ("[T]he reason [a canine sniff of luggage at the airport does] not intrude upon any legitimate privacy interest was that the governmental conduct could reveal nothing about noncontraband items.").

The Supreme Court adopted a similar rationale in United States v. Karo, 468 U.S. 705, 717 (1984). There, the Court held that "[t]he monitoring of a beeper in a private residence, a location not opened to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." Karo, 468 U.S. at 706. The Government argued that "it should be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime is being or will be committed and that monitoring the beeper wherever it goes is likely to produce evidence of criminal activity." Karo, 468 U.S. at 717. In rejecting the Government's argument, the Court explained that "[t]he primary reason for the warrant requirement is to interpose a neutral and detached magistrate between the citizen and the officer engaged in the often competitive enterprise of ferreting out crime," and that "[r]equiring a warrant will have the salutary effect of ensuring that use of beepers is not abused, by imposing upon agents the requirement that they demonstrate in advance their justification for the desired search." Karo, 468 U.S. at 717 (quotations omitted). Thus, even though the DEA believed that the use of the cell-site simulator would reveal the location of a phone associated with criminal activity, the Fourth Amendment requires the Government to obtain a warrant from a neutral magistrate to conduct that search.

The fact that the DEA had obtained a warrant for CSLI from the target cell phone does not change the equation. "If the scope of the search exceeds that permitted by the terms of

a validly issued warrant . . . , the subsequent seizure is unconstitutional without more." Horton v. California, 496 U.S. 128, 140 (1990); see also United States v. Voustianiouk, 685 F.3d 206, 212 (2d Cir. 2012). Here, the use of the cell-site simulator to obtain more precise information about the target phone's location was not contemplated by the original warrant application. If the Government had wished to use a cell-site simulator, it could have obtained a warrant. See Karo, 468 U.S. 705, 718 ("The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement."). And the fact that the Government previously demonstrated probable cause and obtained a warrant for CSLI from Lambis's cell phone suggests strongly that the Government could have obtained a warrant to use a cell-site simulator, if it had wished to do so.

The use of a cell-site simulator constitutes a Fourth Amendment search within the contemplation of Kyllo. Absent a search warrant, the Government may not turn a citizen's cell phone into a tracking device. Perhaps recognizing this, the Department of Justice changed its internal policies, and now requires government agents to obtain a warrant before utilizing a cell-site simulator. See Office of the Deputy Attorney General, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators, 2015 WL 5159600 (Sept. 3, 2015); Deputy Assistant Attorney General Richard Downing Testifies Before House Oversight and Government Reform Committee at Hearing on Geolocation Technology and Privacy, 2016 WL 806338 (Mar. 2, 2016) ("The Department recognizes that the collection of precise location information in real time implicates different privacy interests than less precise information generated by a provider for its business purposes.").

II. Fourth Amendment Considerations

The Government argues that, even if the use of the cell-site simulator constituted

a Fourth Amendment "search," exceptions apply. The Government contends that any taint arising from the search dissipated when the agents gained consent to enter the apartment. The Government also argues that there was no reasonable expectation of privacy under the "third party doctrine."

A. *The Attenuation Doctrine*

Under the attenuation doctrine, "[e]vidence is admissible when the connection between unconstitutional police conduct and the evidence is remote or has been interrupted by some intervening circumstance." Utah v. Strieff, --- S. Ct. ----, 2016 WL 3369419, at *5 (June 20, 2016). In applying the doctrine, courts must determine whether the evidence at issue "was come at by exploitation of that [unconstitutional conduct] or instead by means sufficiently distinguishable to be purged of the primary taint." Wong Sun v. United States, 371 U.S. 471, 488 (1963). The Government maintains that the seizure of evidence from Lambis's apartment was sufficiently attenuated to dissipate the taint from any Fourth Amendment violation because the agents obtained consent from Lambis's father to enter the apartment and obtained consent from Lambis himself to search his bedroom.

However, "the procurement of a 'voluntary' consent to search based upon a prior illegal search may taint the consent." United States v. Tortorello, 533 F.2d 809, 815 (2d Cir. 1976) (citing United States v. Hearn, 496 F.2d 236 (6th Cir. 1974)). "When consent to search is preceded by an unlawful [Fourth Amendment violation], the evidence obtained from the search must ordinarily be suppressed unless the Government shows both that the consent was voluntary and that 'the taint of the initial [seizure] has been dissipated.'" United States v. Murphy, 703 F.3d 182, 190 (2d Cir. 2012) (quoting United States v. Snype, 441 F.3d 119, 132 (2d Cir. 2006)); see also United States v. Cordero-Rosario, 786 F.3d 64, 76–77 (1st Cir. 2015) ("[C]ourts must

determine whether the causal link between a prior unlawful search and consent (voluntary though it may have been) to a subsequent search is so tight that the evidence acquired pursuant to that consent must be suppressed . . . . [T]he fact that the prior unlawful searches by the . . . police led . . . to a . . . party who then consented does not in and of itself show that the taint and exploitation concern simply disappears."); United States v. Washington, 387 F.3d 1060, 1072 n.12 (9th Cir. 2004) ("For purposes of the Fourth Amendment, a determination that a consent was voluntarily made only satisfies a threshold requirement. The mere fact of voluntariness does not mean that a consent is not tainted by a prior Fourth Amendment violation.") (internal quotation marks and citations omitted).

Because the Government obtained consent to enter and search the apartment, the analysis focuses on whether the Fourth Amendment violation was sufficiently attenuated such that obtaining the consent was not an exploitation of the unlawful search. To evaluate attenuation, courts consider four factors: (1) whether the defendant was given Miranda warnings, (2) the temporal proximity of the illegal action to the alleged consent, (3) the presence of intervening circumstances, and (4) the purpose and flagrancy of the official misconduct.[1] Snype, 441 F.3d at 132 (citing Kaupp v. Texas, 538 U.S. 626, 633 (2003)); see also Strieff, 2016 WL 3369419, at *5. Balancing the relevant factors, this Court determines that they weigh in favor of suppression.

The "temporal proximity" factor weighs strongly in favor of suppression. In evaluating this factor, the pertinent question is whether there was sufficient intervening time "to break the chain of illegality." United States v. Ceballos, 812 F.2d 42, 50 (2d Cir. 1987); Murphy, 703 F.3d at 191. Courts "decline[] to find that this factor favors attenuation unless

[1] The first factor is irrelevant to this analysis as consent was not given while the party was in custody. See Snype, 441 F.3d at 134.

'substantial time' elapses." Strieff, 2016 WL 3369419, at *6 (quoting Kaupp, 538 U.S. at 633); see also Brown v. Illinois, 422 U.S. 590, 604 (1975) (finding suppression appropriate where the search occurred "less than two hours" after unconstitutional arrest). Here, the DEA's technician used the cell-site simulator on "the evening of August 27, 2015" (Supp. Tr. at 7) and the agents knocked on Lambis's door at "[a]pproximately 8:00 p.m." of the same evening (Supp. Tr. at 8). In the time leading up to the agents' knock on the apartment door, the technician had to scan the streets surrounding Lambis's apartment complex to identify the correct building and then scan each hallway of the building to identify Lambis's apartment. (Supp. Tr. at 41.)

Based on these facts, this Court finds that the "chain of illegality" was not broken for two reasons. First, although the record is not clear as to the exact amount of time that elapsed between the violation and the consent, the two events were in close temporal proximity. And at least some portion of any time lapse could be attributable to the need for the technician to convey the cell-site simulator results to DEA agents, who then had to come up to the apartment from the street. Second, a surreptitious Fourth Amendment violation should reasonably extend the time necessary to dissipate the taint. Because neither Lambis nor his father were aware of the DEA's use of the cell-site simulator, the DEA could have taken their time in securing consent without much risk that Lambis would dispose of the contraband.

Similarly, the "intervening circumstances" factor supports suppression: no intervening circumstances occurred between the use of the cell-site simulator and the consent to search. As Agent Glover explained, the cell-site simulator led the agents to Lambis's apartment, where they knocked on the door and obtained consent to enter. (Supp. Tr. at 41–42.) Thus, the consent was obtained as a direct result of the illegal Fourth Amendment search and was tainted. Cf. Strieff, 2016 WL 3369419, at *8 (finding intervening circumstance in a valid arrest warrant

that "predated [the officer's] investigation[] and . . . was entirely unconnected with the [unlawful] stop.").

The Sixth Circuit addressed an analogous situation in Hearn. There, the police obtained a search warrant to locate a stolen bulldozer on the defendant's farm. When they arrived at the farm, the defendant was not present. After locating the bulldozer in the first outbuilding they searched, the police then exceeded the scope of the warrant by going on to search a barn 150 yards away. There, the police located a stolen traxcavator. Hearn, 496 F.2d at 239. When the defendant appeared on the scene, police asked him to consent to a search of the barn. Unaware that the police had already entered the barn and discovered the traxcavator, defendant consented to the search. Hearn, 496 F.2d at 242.

The Sixth Circuit held that "information gained by law enforcement officers during an illegal search cannot be used in a derivative manner to obtain other evidence" and set aside the conviction of the defendant on the count relating to the stolen traxcavator. Hearn, 496 F.2d at 244; see also United States v. Hernandez, 279 F.3d 302 (5th Cir. 2002) (prior illegal "squeezing" of defendant's luggage while in luggage compartment of bus, although unknown to defendant, taints subsequent consent because the officer "became sufficiently suspicious to engage [defendant] in conversation" in order to obtain consent to a full search of the luggage); United States v. Cordero-Rosario, 786 F.3d 64, 77 (1st Cir. 2015) (finding relevant "whether absent the illegal search, the investigators would have known the identity of all of the third parties or what to ask them.") (citation and quotations omitted)); United States v. Politano, 491 F. Supp. 456, 463 (W.D.N.Y. 1980) ("[T]he request by Agent Peterson to see the money could only be based upon the information obtained through the prior illegal search at the airport checkpoint by the security personnel and the Cheektowaga police officer."); LaFave, Wayne R.,

Search and Seizure: A Treatise on the Fourth Amendment, § 8.2(d) (5th ed.) (noting that exploitation of a Fourth Amendment violation "may occur by the police taking advantage of earlier illegal acts which are unknown to the consenting party and thus could not have had a coercive effect upon him.") (emphasis in original). Accordingly, the consent obtained by the agents, however voluntary, remained tainted by the Fourth Amendment violation.

The only factor militating in favor of the Government is the "purpose and flagrancy" factor. The Second Circuit has approvingly noted that its "sister circuits have held that purposeful and flagrant police misconduct exists where '(1) the impropriety of the official's misconduct was obvious or the official knew, at the time, that his conduct was likely unconstitutional but engaged in it nevertheless; and (2) the misconduct was investigatory in design and purpose and executed in the hope that something might turn up.'" United States v. Murphy, 703 F.3d 182, 192 (2d Cir. 2012) (quoting United States v. Fox, 600 F.3d 1253, 1261 (10th Cir. 2010)). The DEA agents did not intentionally commit any misconduct. However, the search, "both in design and in execution, was investigatory," Brown, 422 U.S. at 605, and its purpose was clear: identify the apartment unit containing the target phone. As such, this factor only weighs weakly in favor of admission.

B. *The Third Party Doctrine*

Finally, the Government argues for the application of the "third party doctrine." This Court need not address whether the third party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks," United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayer, J., concurring), because even under the historic framework of the doctrine, it is not available to the Government here. The doctrine applies when a party "voluntarily turns over [information] to

third parties." Smith v. Maryland, 442 U.S. 735, 744 (1979); Hoffa v. United States, 385 U.S. 293 (1966) (finding third party doctrine applicable where defendant voluntarily turned over information to Government agent). For instance, in Smith, the Supreme Court found that pen register information is subject to the third party doctrine because "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." Smith, 442 U.S. at 742. However, the location information detected by a cell-site simulator is different in kind from pen register information: it is neither initiated by the user nor sent to a third party.

First, "[c]ell phone users do not actively submit their location information to their service provider." Andrews, 227 Md. App 350 at *25. "When a cell phone is powered up, it acts as a scanning radio, searching through a list of control channels for the strongest signal. The cell phone re-scans every seven seconds or when the signal strength weakens, regardless of whether a call is placed." In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005). These "pings" are sent automatically by the phone to maintain its connection to the network. While the Second Circuit has yet to address whether these passive, CSLI "pings" fall outside the protections of the Fourth Amendment under the third party doctrine,[2] other Circuits have concluded that they do. See United States v. Graham, No. 12-4659, --- F.3d ----, 2016 WL 3068018 (4th Cir. May 31, 2016); United States v.

[2] In an unpublished opinion, the Second Circuit hinted that if presented with the question, it may find that CSLI is not protected by the Fourth Amendment. See United States v. Pascual, 502 F. App'x 75, 80 (2d Cir. 2012) (reviewing under a plain error standard because issue was not raised below and finding that "[i]t certainly was not plain error for the district court not to anticipate this innovative argument and sua sponte exclude the evidence, when no governing precedent from this Court or the Supreme Court required exclusion, and the general principles adopted by those courts pointed the other way"). Courts within the Circuit have tended to find CSLI exempt from the Fourth Amendment. See United States v. Serrano, No. 13-cr-58 (KBF), 2014 WL 2696569, at *7 (S.D.N.Y. June 10, 2014). But see In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113 (E.D.N.Y. 2011) ("[A]n exception to the third-party-disclosure doctrine applies here because cell-phone users have a reasonable expectation of privacy in cumulative cell-site-location records.").

Carpenter, No. 14-1572, 2016 WL 1445183 (6th Cir. Apr. 13, 2016); United States v. Davis, 785 F.3d 498 (11th Cir. 2015); In re U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013). But see In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."); Tracey v. State, 152 So. 3d 504 (Fla. 2014); and State v. Earls, 214 N.J. 564, 583, 70 A.3d 630, 641 (N.J. 2013).

Nevertheless, the arguments that can be made for the application of the third party doctrine to CSLI do not extend to the distinct technology used by a cell-site simulator, which has an additional layer of involuntariness. Unlike CSLI, the "pings" picked up by the cell-site simulator are not transmitted in the normal course of the phone's operation. Rather, "cell site simulators actively locate phones by forcing them to repeatedly transmit their unique identifying electronic serial numbers, and then calculating the signal strength until the target phone is pinpointed." Andrews, 227 Md. App. 350 at *3 n.4 (emphasis added); State v. Tate, 357 Wis. 2d 172, 182 n.8 (Wis. 2014); Department of Justice Policy Guidance: Use of Cell–Site Simulator Technology 2 (Sept. 3, 2015), available at https://www.justice.gov/opa/file/767321/download; Brian L. Owsley, Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions, 66 HASTINGS L.J. 183, 192 (2014) ("[T]here is a vulnerability in the authentication process that enables cell site simulators . . . to breach the system. . . . In other words, the cell site simulator tricks the nearby cell phone into transmitting information to it as it would the nearest cell tower."). The involuntariness of this act is further confirmed by the fact that when the user is actively accessing the network, i.e., placing a call, "the cell site simulator will not be able to access the phone." Andrews, 227 Md. App. 350 at *25. (See also May 23, 2016 Post-

Suppression Hearing Conference Transcript, at 12 ("[I]t is true that when a person is actually speaking into the phone, our cell site simulator cannot send or receive the ping from that phone.").)

Second, unlike pen register information or CSLI, a cell-site simulator does not involve a third party. "Th[e] question of who is recording an individual's information initially is key." In re U.S. for Historical Cell Site Data, 724 F.3d 600, 610 (5th Cir. 2013) (distinguishing between "whether it is the Government collecting the information or requiring a third party to collect and store it, or whether it is a third party, of its own accord and for its own purposes, recording the information"). For both pen register information and CSLI, the Government ultimately obtains the information from the service provider who is keeping a record of the information. With the cell-site simulator, the Government cuts out the middleman and obtains the information directly. Without a third party, the third party doctrine is inapplicable.

CONCLUSION

Lambis's motion to suppress the evidence recovered by DEA agents from his apartment is granted. The Clerk of Court is directed to terminate the motion pending at ECF No. 19.

Dated: July 12, 2016
New York, New York

SO ORDERED:

WILLIAM H. PAULEY III
U.S.D.J.

From: (b)(6); (b)(7)(C)
Sent: 12 Oct 2017 13:55:18 -0400
To: (b)(6); (b)(7)(C)
Subject: Latest cybersmuggling slides
Attachments: Cybersmuggling Investigations (Updated 10.11.17).pptx

Here's the latest version of the Cybersmuggling presentation. There are a couple of new slides, some of which have placeholders for real text so be careful what you copy over. Hope it helps!

(b)(6); (b)(7)(C)

Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (b)(7)(C) (office)
202-731- (mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 17 Nov 2017 10:32:55 -0500
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: News: If NYPD cops want to snoop on your phone, they need a warrant, judge rules

Just a state trial court decision, but thought it was noteworthy.

---

https://arstechnica.com/tech-policy/2017/11/if-nypd-cops-want-to-snoop-on-your-phone-they-need-a-warrant-judge-rules/

If NYPD cops want to snoop on your phone, they need a warrant, judge rules

NY State Supreme Court: Stingrays act as "an instrument of eavesdropping."

CYRUS FARIVAR - 11/17/2017, 5:03 AM

A New York state judge has concluded that a powerful police surveillance tool known as a stingray, a device that spoofs legitimate mobile phone towers, performs a "search" and therefore requires a warrant under most circumstances.

As a New York State Supreme Court judge in Brooklyn ruled earlier this month in an attempted murder case, New York Police Department officers should have sought a standard, probable cause-driven warrant before using the invasive device.

The Empire State court joins others nationwide in reaching this conclusion. In September, the District of Columbia Court of Appeals also found that stingrays normally require a warrant, as did a federal judge in Oakland, California, back in August.

According to *The New York Times*, which first reported the case on Wednesday, *People v. Gordon* is believed to be the first stingray-related case connected to the country's largest city police force.

"By its very nature, then, the use of a cell site simulator intrudes upon an individual's reasonable expectation of privacy, acting as an instrument of eavesdropping and requires a separate warrant

supported by probable cause rather than a mere *pen register/trap and trace* order such as the one obtained in this case by the *NYPD,"* Justice Martin Murphy wrote in the November 3 decision.

A "pen register" warrant, sometimes known as a "pen/trap order," which typically only provides a call log for a particular number, has been used in the era of stingrays to also include location information. Historically, law enforcement officers nationwide have not been forthright with judges when explaining what the devices do.

As Ars has long reported, stingrays can be used to determine a mobile phone's location by spoofing a cell tower. In some cases, stingrays can also intercept calls and text messages. Once deployed, the devices intercept data from a target phone along with information from other phones within the vicinity. At times, police have falsely claimed the use of a confidential informant when they have actually deployed these particularly sweeping and intrusive surveillance tools.

In this case, the suspect, Shuquan Gordon, was located in a Brooklyn apartment building seemingly out of nowhere. This was "an address not previously identified as of any interest to this investigation," as the judge noted.

Brian Owsley, a law professor at the University of North Texas and a former federal magistrate judge, whose 2014 law review article on stingrays was cited numerous times by the Brooklyn judge, told Ars that this ruling fell in line with what he called "positive momentum" toward proper regulation.

"There is still a long way to go," he e-mailed. "Moreover, as good as this decision is, the current progress is more aptly described as two steps forward followed by one step back."

(b)(6); (b)(7)(C)

Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (b)(7)(C) (office)
202-731-(b)(6); (b)(7)(C) (mobile)
(b)(6); (b)(7)(C)

document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 17:33:08 +0000
To: (b)(6); (b)(7)(C)
Subject: question on Stingrays

(b)(6); (b)(7)(C)

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

Thanks, (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
(202) 732 (b)(6); (b)(7)(C) (office)
(202) 308 (cell)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 26 Aug 2016 18:25:07 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: Cell-site Simulator for Palms
Attachments: ICE draft memo Use of Cell-Site Simulator Technology.doc

(b)(6); (b)(7)(C)

(b)(5); (b)(7)(E)

All the best,

(b)(6);
(b)(7)(C)

(b)(6); (b)(7)(C)

Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (b)(7)(C) (office)
202-500- (mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Tuesday, August 23, 2016 12:00 PM
To: (b)(6); (b)(7)(C)
Subject: RE: Cell-site Simulator for Palms

(b)(6);
(b)(7)(C)

(b)(6);
(b)(7)(C) wanted us to put in some FAQs at the end of the power point. When you have a moment, can you please take a look and let me know if you have any objections?

(b)(5); (b)(7)(E)

Thanks,

(b)(6); (b)(7)(C)

Section Chief / Supervisory Special Agent

Homeland Security Investigations
Technical Operations Unit - Investigative Intercept Section
(b)(6); (b)(7)(C)

Lorton, VA 22079
703-551-[redacted] Office)
716-510-[redacted] Cell)
[redacted]

From: [redacted]
Sent: Monday, August 22, 2016 6:39 PM
To: [redacted]
Subject: RE: Cell-site Simulator for Palms

Okay, will do.

[redacted]
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-[redacted] (office)
202-500-[redacted] (mobile)
[redacted]

From: [redacted]
Sent: Monday, August 22, 2016 6:29:14 PM
To: [redacted]
Subject: RE: Cell-site Simulator for Palms

[redacted]

I believe that once it gets the blessing from HSI policy, it will be sent to you for your official review. If you have anything that you feel should be edited, I can make the modifications prior to sending it back to policy. That may make it easier for the process in the long run…

Thanks,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Section Chief / Supervisory Special Agent

Homeland Security Investigations
Technical Operations Unit - Investigative Intercept Section
(b)(6); (b)(7)(C)
Lorton, VA 22079
703-551 (b)(6); (b)(7)(C) (Office)
716-510 (Cell)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, August 22, 2016 6:27 PM
To: (b)(6); (b)(7)(C)
Subject: RE: Cell-site Simulator for Palms

Thanks (b)(6); (b)(7)(C) do you need an official review of this from our office, or just an informal opinion?

(b)(5); (b)(7)(E)

Sincerely,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732 (b)(6); (b)(7)(C) (office)
202-500 (mobile)
(b)(6); (b)(7)(C)

disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

From: (b)(6); (b)(7)(C)
Sent: Monday, August 22, 2016 6:16 PM
To: (b)(6); (b)(7)(C)
Subject: RE: Cell-site Simulator for Palms

(b)(6); (b)(7)(C)

Attached is the draft. I have a few edits to make before sending it back to HSI policy. Please take a look and let me know what you think. I'll let Policy know that you're our POC on this project.

Thanks again,

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, August 22, 2016 6:04 PM
To: (b)(6); (b)(7)(C)
Subject: RE: Cell-site Simulator for Palms

Hi (b)(6);

I just wanted to see if you had your hands on a copy of the HSI policy. Thanks a lot,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (b)(7)(C) office)
202-500(b) mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Friday, August 19, 2016 10:06 AM

To: (b)(6); (b)(7)(C)
Subject: RE: Cell-site Simulator for Palms

There's an HSI draft, which is almost identical to the DHS version, which has not yet been signed by the EAD. I met with HSI policy last week for some edits. I'll send you a copy on Monday, to make sure you're in the loop.

Thanks,

(b)(6); (b)(7)(C)

Take care,

(b)(6); (b)(7)(C)
Section Chief / Supervisory Special Agent

Homeland Security Investigations
Technical Operations Unit - Investigative Intercept Section
10450 Furnace Road
Lorton, VA 22079
703-551 (b)(6); (b)(7)(C) (Office)
716-510 (Cell)
(b)(6); (b)(7)(C)

From (b)(6); (b)(7)(C)
Sent: Friday, August 19, 2016 10:02:11 AM
To (b)(6); (b)(7)(C)
Subject: RE: Cell-site Simulator for Palms

The actual policy from DHS or the ICE policy just recently signed? I wasn't involved in either, before my time as well, but I may know who was. However, I am now the POC on this along with (b)(6); (b)(7)(C)

Best,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Associate Legal Advisor

Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-[redacted] (Office)
202-500-[redacted] (Mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Friday, August 19, 2016 9:36:51 AM
To: (b)(6); (b)(7)(C)
Subject: RE: Cell-site Simulator for Palms

(b)(6); (b)(7)(C)

(b)(5)

Thanks,

(b)(6); (b)(7)(C)

Take care,

(b)(6); (b)(7)(C)

Section Chief / Supervisory Special Agent

Homeland Security Investigations
Technical Operations Unit - Investigative Intercept Section
(b)(6); (b)(7)(C)
Lorton, VA 22079

703-551-[redacted] (Office)
716-510-[redacted] (Cell)
[redacted]

From: [redacted]
Sent: Friday, August 19, 2016 9:25:11 AM
To: [redacted]
Subject: Cell-site Simulator for Palms

[redacted]

I reviewed the PPT you sent me and I made a bunch of edits and comments. It is with my management for approval. I'm hoping I get it back by today, but it may be early next week.

Sincerely,

[redacted]

[redacted]
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-[redacted] (office)
202-500-[redacted] (mobile)
[redacted]

Homeland Security Investigations
Office of the Executive Associate Director

U.S. Department of Homeland Security
500 12th Street, SW
Washington, D.C. 20536

U.S. Immigration and Customs Enforcement

(b)(5); (b)(7)(E)

MEMORANDUM FOR: Assistant Directors
Deputy Assistant Director
Special Agents in Charge
Attachés

FROM: Peter T. Edge
Executive Associate Director

SUBJECT: Use of Cell-Site Simulator Technology

Purpose:

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

~~LAW ENFORCEMENT SENSITIVE~~

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

From: (b)(6); (b)(7)(C)
Sent: 6 Jun 2017 18:05:31 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: 3L?

I am and I am (only thing I see that day is one of the Cell-site Simulator trainings at Tech Ops but I'm not presenting any of those).

Thanks,

(b)(6);

From: (b)(6); (b)(7)(C)
Sent: Tuesday, June 06, 2017 2:01 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: 3L?

You betcha! You up for it? You available that day?

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6);
202-538-(b)(7)(C) iPhone)

***** Warning *** Attorney/Client Privilege *** Attorney Work Product *****
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From: (b)(6); (b)(7)(C)
Sent: Tuesday, June 6, 2017 1:59 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: 3L?

A 3L w/ CALD on WSE?

From: (b)(6); (b)(7)(C)
Sent: Tuesday, June 06, 2017 1:58 PM
To: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 9 May 2017 15:50:01 -0400
To: (b)(6); (b)(7)(C)
Subject: RE: 5/25 (b) (7)(E) visit

(b)(6);

Absolutely. I am here usually everyday by 7:30 a.m. Just give me a heads up the night before you plan to arrive for the day so I can plan accordingly. Right now, that carrel outside of (b)(6); old office is being used, but I'm sure we can find a place for you.

Waiting on next stage for that TIII WG. The draft "present day" breakdown of operations and staffing has been circulated for review and comments. I'll let you know what else comes up.

Thanks -

SA (b)(6); (b)(7)(C)
HSI Title-III Investigative Programs
(202) 359-(b)(6);

From: (b)(6); (b)(7)(C)
Sent: Tuesday, May 9, 2017 3:37 PM
To: (b)(6); (b)(7)(C)
Subject: 5/25 (b) (7)(E) visit

(b)(6);

Let me know if OPLA can assist in any way on the TIII WG at this stage.

Also, I was on a schedule to spend a day over at (b) (7)(E) each month (sometimes 2). I would usually use the carrel outside (b)(6); (b)(7)(office but if that was being used I could usually find a carrel / conference room to sit in.

I am scheduled to come to (b) (7)(E) for Cell Site Simulator training on 5/25. I would like to spend the entire day out there (training is at 1 p.m.; I live in Springfield so not really worth going back and forth to PCN).

Let me know if I can work that out through you on 5/25 and in the future – I think (b)(6); had to let someone at the downstairs desk I'm was coming.

Thanks, (b)(6);

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement

(202) 732-(b)(6) (office)
(202) 308-(b)(7) (cell)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 19 Apr 2017 16:28:51 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: Cell-Site Simulator training to the client

Works for me.

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (b)(7)(C) Desk)
202-536-(b)(6); (b)(7)(C) Cell)

From: (b)(6); (b)(7)(C)>
Date: Wednesday, Apr 19, 2017, 4:16 PM
To: (b)(6); (b)(7)(C)
Cc:
<(b)(6); (b)(7)(C)>
Subject: FW: Cell-Site Simulator training to the client

(b)(6);

Can I work from Tech Ops on 5/25?

Thanks, (b)(6);

From: (b)(6); (b)(7)(C)
Sent: Wednesday, April 19, 2017 2:39 PM
To: (b)(6); (b)(7)(C)

Cc: (b)(6); (b)(7)(C)
Subject: Cell-Site Simulator training to the client

(b) (7)(E) eam,

We have been asked to provide an hour long training on ICE's cell-site simulator policy on behalf of Tech-Ops to its field TEOs. There are four sessions that will be held this summer at the Lorton VA facility. After discussing with (b)(6); and (b)(6); (b)(7)(C) the following was decided:

On Thursday May 25th, from 11-12, all of the Tech Ops team will travel to Lorton and watch me give the presentation on cell-site simulators.

On Thursday, June 8th, from 11-12, (b)(6); will give the presentation and (b)(6) will join him.

On Thursday June 26th, from 11-12, Will will give the presentation and (b)(6); will join him.

On Thursday July 27th, from 11-12, either (b)(6) or (b)(6); will give the presentation, and it can be left to the two of you to decide who will go.

I believe the presentation and policy is on the S:Drive, and if it isn't, I will make sure it is this afternoon. Please let me know if you have any questions or comments, calendar invites will be forthcoming.

Sincerely,

(b)(6);

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); office)
202-500-(b)(7)(mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 28 Mar 2019 15:27:04 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: DTAS Legal Block of Instruction
Attachments: DTAS 901 Schedule.xls

See attached. We have you presenting at 1-4 p.m. on Tuesday 4/2/19.

(b)(6); (b)(7)(C) | Program Manager
Advanced Training / HSI Academy
Federal Law Enforcement Training Center, Glynco, GA 31524
Office: 912.267.(b)(6); iPhone: 520.631.(b)(6); (b)(6); (b)(7)(C)
Homeland Security

From: (b)(6); (b)(7)(C)
Sent: Thursday, March 28, 2019 11:22 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: DTAS Legal Block of Instruction

Thank you (b)(6); Working on it now. Can you please send me the agenda and during what time block I will be presenting?

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
(202) 732-(b)(6); office)
(716) 553-(b)(7)(C) cell)

From (b)(6); (b)(7)(C)
Sent: Thursday, March 28, 2019 11:20 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: DTAS Legal Block of Instruction

(b)(6);

Good morning. If you can, submit your travel authorization today. Refer to trip as Guest Instructor for DTAS-901. This is a way for us to track. The authorization will need to be approved by your supervisor and a MSS at the Academy will fund and complete the authorization. Let me know when you submit it and if you have any questions.

Thank you for assisting with this class.

(b)(6); (b)(7)(C) | Program Manager
Advanced Training / HSI Academy
Federal Law Enforcement Training Center, Glynco, GA 31524
Office: 912.267(b)(6); | iPhone: 520.631(b)(6); | (b)(6); (b)(7)(C)
Homeland Security

From: (b)(6); (b)(7)(C)
Sent: Wednesday, March 27, 2019 2:50 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: DTAS Legal Block of Instruction

Hi (b)(6);

CLS attorney (b)(6); (b)(7)(C) (cc'd here) will be coming to FLETC to present the OPLA block of DTAS.

To confirm, Monday (4/1) and Wednesday (4/3) are travel days w/ (b)(6); (b)(7)(C) presenting a three (3) hour block of instruction on Tuesday 4/2.

Please send the funding string to (b)(6); as soon as possible.

Can you also please send her the current agenda and any other information she needs prior to traveling to FLETC?

Thanks!

(b)(6);

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
(202) 732-(b)(6) (office)
(202) 308-; (cell)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Tuesday, March 26, 2019 4:29 PM
To: (b)(6); (b)(7)(C)
Subject: DTAS Legal Block of Instruction

(b)(6);

Good afternoon. We have a DTAS class scheduled to start next week. I've been dealing with a lot of different classes issues here and I completely forgot to reach out to you and check your availability for next Tuesday April 2. Please give me a call when you return to the office tomorrow.

Take care,

(b)(6); (b)(7)(C) | Program Manager
Advanced Training / HSI Academy
Federal Law Enforcement Training Center, Glynco, GA 31524
Office: 912.267(b)(6); | iPhone: 520.631(b)(6); | (b)(6); (b)(7)(C)
Homeland Security

DHS, Homeland Security Investigations Academy 3/28/2019

Federal Law Enforcement Training Center- Glynco, GA Designated Technical Agent School 1901

Bldg 65 Room 202 Class Coordinator: (b)(6); (b)(7)(C) Week 1

TIME	Monday 4/1	Tuesday 4/2	Wednesday 4/3	Thursday 4/4	Friday 4/5	Saturday 4/6
8:00		Welcome	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)		
	Students	HSI Academy Management				
9:00	TRAVEL DAY	(b)(6); (b)(7)(C)				
9:00		Orientation / Administra	(Hands-on)			
		Program Ovierview				
10:00		(b)(6); (b)(7)(C)				
10:00		TechOps Presentation	(b)(5); (b)(7)(E)			
	Instructors					
11:00	CLASS PREPARATION	(b)(6); (b)(7)(C)	(PowerPoint)			
11:00		(b)(5); (b)(7)(E) Training				
12:00		(b)(6); (b)(7)(C)				
Lunch						
1:00		Legal	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	
	Students	4th Amendment			(Lecture and Hands-on)	
2:00	TRAVEL DAY	Electronic Surveillance Law				
2:00			(b)(5); (b)(7)(E)			
			(Hands-on and Project)			
3:00				(b)(6); (b)(7)(C)		
3:00				(b)(5); (b)(7)(E)	Cell-Site Simulator	
	Instructors	(b)(6); (b)(7)(C)		(Hands-on)	(Lecture)	
4:00	CLASS PREPARATION	HQ OPLA Associate Legal Advisor				
4:00		(b)(5); (b)(7)(E)				
5:00		(b)(6); (b)(7)(C)				
5:00 AFTER HOURS 6:30						

Notes:

APPROVED, (Title of Approving Official) _____

DHS, Homeland Security Investigations Academy

3/28/2019

Federal Law Enforcement Training Center- Glynco, GA

Designated Technical Agent School

Bldg. 65 Room 202 Class Coordinator: (b)(6); (b)(7)(C)

Week 2

TIME	Monday 4/8	Tuesday 4/9	Wednesday	Thursday 4/10	Friday 4/12	Saturday 4/13
8:00	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	Final Practical Exerci	(b)(5); (b)(7)(E) Overview	
9:00		(Hands-on)		Group A	(b)(6); (b)(7)(C)	TRAVEL DAY
9:00	(Hands-on)			(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	
10:00			(b)(6); (b)(7)(C)			
10:00			(b)(5); (b)(7)(E)			
			(Hands-on)	Group B		
11:00				(b)(5); (b)(7)(E)		
11:00						
12:00	(b)(6); (b)(7)(C)			All Instructors	(b)(6); (b)(7)(C)	
Lunch						
1:00	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	(b)(5); (b)(7)(E)	Final Practical Exerci	Course	
					(b)(5); (b)(7)(E)	
2:00		(Hands-on)		Group B		
2:00				(b)(5); (b)(7)(E)		
	(Hands-on)	Optional Project				
3:00		(b)(5); (b)(7)(E)	(b)(6); (b)(7)(C)		All Instructors	
3:00			(b)(5); (b)(7)(E)		GRADUATION	
				Group A		
4:00				(b)(5); (b)(7)(E)		
4:00						
5:00	(b)(6); (b)(7)(C)			All Instructors		
5:00 AFTER HOURS			(b)(5); (b)(7)(E)			
6:30			All Instructors			

Notes: Breakout Rooms

APPROVED, (Title of Approving Official) _____

From: (b)(6); (b)(7)(C)
Sent: 22 Sep 2017 13:08:38 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

1) Not HSI.
2) DC Metropolitan Police Department (MPD).
3) *Jones v. United States*, No. 15-CF-322 (D.C. Cir. Sept. 21, 2017) *[strange citation since not case not yet published in a reporter]*

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) (Desk)
202-839-(b)(7)(C) (Cell)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:42 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

Hit send too soon. Two questions:

1) This was not an HSI case, right? What agency was it?

2) Can you please send me the cite?

I know. That's three questions. But I only had two numbers so back off. Thanks.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6);
202-538-(b)(7)(C) (iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:40 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

Thank you both.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6);
202-538-(b)(7)(C) (iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:33 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) (Desk)
202-839-(b)(7) (Cell)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:06 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5)

(b)(5)

Sent with BlackBerry Work (www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Sep 22, 2017, 10:41 AM
To: (b)(6); (b)(7)(C),
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(are asking.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732(b)(6);
202-538(b)(7)(iPhone)

***** Warning *** Attorney/Client Privilege *** Attorney Work Product *****
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:43 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6);
202-538-(b)(7)(iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:38 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

Police use of 'StingRay' cellphone tracker requires search warrant, appeals court rules

By Tom Jackman September 21 at 5:20 PM

<< OLE Object: Picture (Device Independent Bitmap) >>

A "StingRay II," made by the Harris Corp., can redirect cellphone calls away from cell tower antennae and capture their identifying data and location. Police use them to find people. Some argue that that's an invasion of privacy. (Courtesy Harris Corp.)

A device that tricks cellphones into sending it their location information and has been used quietly by policeand federal agents for

years, requires a search warrant before it is turned on, an appeals court in Washington ruled Thursday. It is the fourth such ruling by either a state appeals court or federal district court, and may end up deciding the issue unless the government takes the case to the U.S. Supreme Court or persuades the city's highest court to reverse the ruling.

The case against Prince Jones in 2013 involved D.C. police use of a "StingRay" cell-site simulator, which enables law enforcement to pinpoint the location of a cellphone more precisely than a phone company can when triangulating a signal between cell towers or using a phone's GPS function. Civil liberties advocates say the StingRay, by providing someone's location to police without court approval, is a violation of an individual's Fourth Amendment right not to be unreasonably searched. The D.C. Court of Appeals agreed in a 2 to 1 ruling, echoing similar rulings in the Maryland Court of Special Appeals and federal district courts in New York City and San Francisco.

"This opinion," said Nathan F. Wessler of the American Civil Liberties Union, who helped argue the case with the D.C. Public Defender Service, "joins the growing chorus of courts holding that the Fourth Amendment protects against warrantless use of invasive, covert technology to track people's phones. … We applaud today's opinion for erecting sensible and strong protections against the government violating people's privacy in the digital age."

The U.S. attorney's office in Washington declined to comment on the ruling. The prosecutors could ask for a rehearing by the three judge panel or the entire appeals court, and if those are denied take the case to the Supreme Court, though Wessler noted that the high court might not be inclined to take a case where there is no dispute among the lower court rulings.

The Justice Department issued policy guidance to its agencies in 2015 that a search warrant must be obtained for all StingRay uses, and though that is not binding on state and local police, the Metropolitan Police Department has said it would abide by that rule. The ACLU has counted 72 cell-site simulators in use in 24 states and the District, but

believes there could be many more. Both D.C. and Baltimore police had signed an agreement with the FBI not to disclose or discuss their StingRay device publicly, court records show, and an FBI agent sat with prosecutors during Jones's trial to advise them on how to handle questions about the device.

The ruling by the D.C. Court of Appeals resulted in all the evidence in the case against Jones being thrown out, and a nine-count felony conviction for sexual abuse, kidnapping, armed robbery and threats being vacated.

Jones was arrested after he allegedly assaulted and robbed two women in separate incidents, after arranging to meet with them through Backpage.com for sexual liaisons. In both cases, the perpetrator took the victims' cellphones.

After the second incident, D.C. police compared the call records of the victims and found that the same phone number had been used to arrange both meetings. The police then obtained the mobile identification number for the man's phone, as well as the identification numbers for the victims' phones, and with the help of the phone companies obtained a general location for the phones, which police said appeared to be traveling together.

Once in the vicinity of the phones, the police turned on the StingRay, court records show, and punched in the identification number (different from the phone number) of the assailant's phone. The StingRay acts like a cell site antenna, and convinces cellphones to connect to it instead of a real cell site, providing the phone numbers and locations of the phones that connect. The phones are useless during this time because they aren't connected to an actual network, only the StingRay.

Before long, the assailant's prepaid cellphone was found on Jones, sitting in a parked car on Minnesota Avenue in Northeast Washington, as were the phones stolen from the victims, police said. The appeals court ruled, and the defense agreed, that if the police had used the StingRay on one of the victims' phones, instead of Jones's phone, the

search would have been legal because the victims consented to the search.

The judge in Jones's trial declined to suppress the phone seizure, which in turn led to the knife apparently used in the robberies, the discovery of the victims' phones and incriminating statements made by Jones and his girlfriend. But the ruling written by Associate Judge Corinne A. Beckwith, joined by Senior Judge Michael W. Farrell, threw out all of that evidence as "fruit of the poisonous tree," namely the StingRay.

"Locating and tracking a cell-site simulator," Beckwith wrote, "has the substantial potential to expose the owner's intimate personal information," particularly their movements and whereabouts. "A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will."

For that reason, Beckwith said, "the use of a cell-site simulator to locate Mr. Jones's phone invaded a reasonable expectation of privacy and was thus a search."

Prosecutors argued that everyone knows that the location of a cellphone can be tracked, and at oral argument one noted that every fleeing criminal on television dramas throws away or destroys their phone. Beckwith disregarded that approach, saying that "a person does not lose a reasonable expectation of privacy merely because he or she is made aware of the government's capacity to invade his or her privacy."

Associate Judge Phyllis D. Thompson dissented, though she wrote that under ordinary circumstances, she agreed that the government's use of a StingRay "likely violates the legitimate expectation of privacy." But Thompson said Jones forfeited that privacy when he drove around with the victims' stolen cellphones. Beckwith responded that Jones had not been charged or convicted of stealing the phones at the time of the search.

The StingRay issue is separate from another cellphone issue pending before the Supreme Court — whether law enforcement must obtain a warrant before obtaining a cellphone's historical location data from a phone company. Phone companies record which cell towers are used when a call is made, which police often use to demonstrate a person's whereabouts at the time of a crime. Those records can be obtained with a court order, and a lower standard of proof, rather than a warrant. The ACLU's Wessler said that Thursday's ruling was a "recognition that constitutional protections must keep pace with advancing technology, and is an important reminder of what is at stake as the Supreme Court takes up the issue of police requests for historical cellphone location data."

From: (b)(6); (b)(7)(C)
Sent: 22 Sep 2017 12:41:56 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

Hit send too soon. Two questions:

1) This was not an HSI case, right? What agency was it?

2) Can you please send me the cite?

I know. That's three questions. But I only had two numbers so back off. Thanks.

(b)(6); (b)(7)(C) berta
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C)
202-538- (iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:40 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

Thank you both.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C)
202-538- (iPhone)

From: (b)(6);
Sent: Friday, September 22, 2017 12:33 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (Desk)
202-839-(b)(7)(C) (Cell)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:06 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5)

Sent with BlackBerry Work (www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Sep 22, 2017, 10:41 AM
To: (b)(6); (b)(7)(C),
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); are asking.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732(b)(6);
202-538(b)(7)(iPhone)

From: Liberta, Joseph M
Sent: Friday, September 22, 2017 9:43 AM
To: Laytin, Alexander; Burke, Sean P; Harrold, Marc M; Rubens, William B
Cc: Beck Tokoph, Anne (Anne.BeckTokoph@ice.dhs.gov); Falcone, Michael
Subject: FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C)
202-538- (iPhone)

From: Davis, Mike P
Sent: Friday, September 22, 2017 9:38 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

Police use of 'StingRay' cellphone tracker requires

search warrant, appeals court rules

By Tom Jackman September 21 at 5:20 PM

<< OLE Object: Picture (Device Independent Bitmap) >>

A "StingRay II," made by the Harris Corp., can redirect cellphone calls away from cell tower antennae and capture their identifying data and location. Police use them to find people. Some argue that that's an invasion of privacy. (Courtesy Harris Corp.)

A device that tricks cellphones into sending it their location information and has been used quietly by policeand federal agents for years, requires a search warrant before it is turned on, an appeals court in Washington ruled Thursday. It is the fourth such ruling by either a state appeals court or federal district court, and may end up deciding the issue unless the government takes the case to the U.S. Supreme Court or persuades the city's highest court to reverse the ruling.

The case against Prince Jones in 2013 involved D.C. police use of a "StingRay" cell-site simulator, which enables law enforcement to pinpoint the location of a cellphone more precisely than a phone company can when triangulating a signal between cell towers or using a phone's GPS function. Civil liberties advocates say the StingRay, by providing someone's location to police without court approval, is a violation of an individual's Fourth Amendment right not to be unreasonably searched. The D.C. Court of Appeals agreed in a 2 to 1 ruling, echoing similar rulings in the Maryland Court of Special Appeals and federal district courts in New York City and San Francisco.

"This opinion," said Nathan F. Wessler of the American Civil Liberties Union, who helped argue the case with the D.C. Public Defender Service, "joins the growing chorus of courts holding that the Fourth Amendment protects against warrantless use of invasive, covert technology to track people's phones. … We applaud today's opinion for erecting sensible and strong protections against the government violating people's privacy in the digital age."

The U.S. attorney's office in Washington declined to comment on the ruling. The prosecutors could ask for a rehearing by the three judge panel or the entire appeals court, and if those are denied take the case to the Supreme Court, though Wessler noted that the high court might not be inclined to take a case where there is no dispute among the lower court rulings.

The Justice Department issued policy guidance to its agencies in 2015 that a search warrant must be obtained for all StingRay uses, and though that is not binding on state and local police, the Metropolitan Police Department has said it would abide by that rule. The ACLU has counted 72 cell-site simulators in use in 24 states and the District, but believes there could be many more. Both D.C. and Baltimore police had signed an agreement with the FBI not to disclose or discuss their StingRay device publicly, court records show, and an FBI agent sat with prosecutors during Jones's trial to advise them on how to handle questions about the device.

The ruling by the D.C. Court of Appeals resulted in all the evidence in the case against Jones being thrown out, and a nine-count felony conviction for sexual abuse, kidnapping, armed robbery and threats being vacated.

Jones was arrested after he allegedly assaulted and robbed two women in separate incidents, after arranging to meet with them through Backpage.com for sexual liaisons. In both cases, the perpetrator took the victims' cellphones.

After the second incident, D.C. police compared the call records of the victims and found that the same phone number had been used to arrange both meetings. The police then obtained the mobile identification number for the man's phone, as well as the identification numbers for the victims' phones, and with the help of the phone companies obtained a general location for the phones, which police said appeared to be traveling together.

Once in the vicinity of the phones, the police turned on the StingRay, court records show, and punched in the identification number (different from the phone number) of the assailant's phone. The

StingRay acts like a cell site antenna, and convinces cellphones to connect to it instead of a real cell site, providing the phone numbers and locations of the phones that connect. The phones are useless during this time because they aren't connected to an actual network, only the StingRay.

Before long, the assailant's prepaid cellphone was found on Jones, sitting in a parked car on Minnesota Avenue in Northeast Washington, as were the phones stolen from the victims, police said. The appeals court ruled, and the defense agreed, that if the police had used the StingRay on one of the victims' phones, instead of Jones's phone, the search would have been legal because the victims consented to the search.

The judge in Jones's trial declined to suppress the phone seizure, which in turn led to the knife apparently used in the robberies, the discovery of the victims' phones and incriminating statements made by Jones and his girlfriend. But the ruling written by Associate Judge Corinne A. Beckwith, joined by Senior Judge Michael W. Farrell, threw out all of that evidence as "fruit of the poisonous tree," namely the StingRay.

"Locating and tracking a cell-site simulator," Beckwith wrote, "has the substantial potential to expose the owner's intimate personal information," particularly their movements and whereabouts. "A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will."

For that reason, Beckwith said, "the use of a cell-site simulator to locate Mr. Jones's phone invaded a reasonable expectation of privacy and was thus a search."

Prosecutors argued that everyone knows that the location of a cellphone can be tracked, and at oral argument one noted that every fleeing criminal on television dramas throws away or destroys their phone. Beckwith disregarded that approach, saying that "a person does not lose a reasonable expectation of privacy merely because he or

she is made aware of the government's capacity to invade his or her privacy."

Associate Judge Phyllis D. Thompson dissented, though she wrote that under ordinary circumstances, she agreed that the government's use of a StingRay "likely violates the legitimate expectation of privacy." But Thompson said Jones forfeited that privacy when he drove around with the victims' stolen cellphones. Beckwith responded that Jones had not been charged or convicted of stealing the phones at the time of the search.

The StingRay issue is separate from another cellphone issue pending before the Supreme Court — whether law enforcement must obtain a warrant before obtaining a cellphone's historical location data from a phone company. Phone companies record which cell towers are used when a call is made, which police often use to demonstrate a person's whereabouts at the time of a crime. Those records can be obtained with a court order, and a lower standard of proof, rather than a warrant. The ACLU's Wessler said that Thursday's ruling was a "recognition that constitutional protections must keep pace with advancing technology, and is an important reminder of what is at stake as the Supreme Court takes up the issue of police requests for historical cellphone location data."

From: (b)(6); (b)(7)(C)
Sent: 22 Sep 2017 12:39:50 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

Thank you both.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C)
202-538-(iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:33 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section

Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (b)(7)(C) Desk)
202-839-(b)(6); (b)(7)(C) Cell)

From (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:06 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5)

Sent with BlackBerry Work (www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Sep 22, 2017, 10:41 AM
To: (b)(6); (b)(7)(C),
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(are asking.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6);

202-538-(b)(6); (b)(7)(C) (iPhone)

***** Warning *** Attorney/Client Privilege *** Attorney Work Product *****
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:43 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C)
202-538-(b)(6); (b)(7)(C) (iPhone)

***** Warning *** Attorney/Client Privilege *** Attorney Work Product *****
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:38 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

Police use of 'StingRay' cellphone tracker requires search warrant, appeals court rules

By Tom Jackman September 21 at 5:20 PM

<< OLE Object: Picture (Device Independent Bitmap) >>

A "StingRay II," made by the Harris Corp., can redirect cellphone calls away from cell tower antennae and capture their identifying data and location. Police use them to find people. Some argue that that's an invasion of privacy. (Courtesy Harris Corp.)

A device that tricks cellphones into sending it their location information and has been used quietly by policeand federal agents for years, requires a search warrant before it is turned on, an appeals court in Washington ruled Thursday. It is the fourth such ruling by either a state appeals court or federal district court, and may end up deciding the issue unless the government takes the case to the U.S. Supreme Court or persuades the city's highest court to reverse the ruling.

The case against Prince Jones in 2013 involved D.C. police use of a "StingRay" cell-site simulator, which enables law enforcement to pinpoint the location of a cellphone more precisely than a phone company can when triangulating a signal between cell towers or using a phone's GPS function. Civil liberties advocates say the StingRay, by providing someone's location to police without court approval, is a violation of an individual's Fourth Amendment right not to be unreasonably searched. The D.C. Court of Appeals agreed in a 2 to 1

ruling, echoing similar rulings in the Maryland Court of Special Appeals and federal district courts in New York City and San Francisco.

“This opinion,” said Nathan F. Wessler of the American Civil Liberties Union, who helped argue the case with the D.C. Public Defender Service, “joins the growing chorus of courts holding that the Fourth Amendment protects against warrantless use of invasive, covert technology to track people’s phones. … We applaud today’s opinion for erecting sensible and strong protections against the government violating people’s privacy in the digital age.”

The U.S. attorney’s office in Washington declined to comment on the ruling. The prosecutors could ask for a rehearing by the three judge panel or the entire appeals court, and if those are denied take the case to the Supreme Court, though Wessler noted that the high court might not be inclined to take a case where there is no dispute among the lower court rulings.

The Justice Department issued policy guidance to its agencies in 2015 that a search warrant must be obtained for all StingRay uses, and though that is not binding on state and local police, the Metropolitan Police Department has said it would abide by that rule. The ACLU has counted 72 cell-site simulators in use in 24 states and the District, but believes there could be many more. Both D.C. and Baltimore police had signed an agreement with the FBI not to disclose or discuss their StingRay device publicly, court records show, and an FBI agent sat with prosecutors during Jones’s trial to advise them on how to handle questions about the device.

The ruling by the D.C. Court of Appeals resulted in all the evidence in the case against Jones being thrown out, and a nine-count felony conviction for sexual abuse, kidnapping, armed robbery and threats being vacated.

Jones was arrested after he allegedly assaulted and robbed two women in separate incidents, after arranging to meet with them through Backpage.com for sexual liaisons. In both cases, the perpetrator took the victims’ cellphones.

After the second incident, D.C. police compared the call records of the victims and found that the same phone number had been used to arrange both meetings. The police then obtained the mobile identification number for the man's phone, as well as the identification numbers for the victims' phones, and with the help of the phone companies obtained a general location for the phones, which police said appeared to be traveling together.

Once in the vicinity of the phones, the police turned on the StingRay, court records show, and punched in the identification number (different from the phone number) of the assailant's phone. The StingRay acts like a cell site antenna, and convinces cellphones to connect to it instead of a real cell site, providing the phone numbers and locations of the phones that connect. The phones are useless during this time because they aren't connected to an actual network, only the StingRay.

Before long, the assailant's prepaid cellphone was found on Jones, sitting in a parked car on Minnesota Avenue in Northeast Washington, as were the phones stolen from the victims, police said. The appeals court ruled, and the defense agreed, that if the police had used the StingRay on one of the victims' phones, instead of Jones's phone, the search would have been legal because the victims consented to the search.

The judge in Jones's trial declined to suppress the phone seizure, which in turn led to the knife apparently used in the robberies, the discovery of the victims' phones and incriminating statements made by Jones and his girlfriend. But the ruling written by Associate Judge Corinne A. Beckwith, joined by Senior Judge Michael W. Farrell, threw out all of that evidence as "fruit of the poisonous tree," namely the StingRay.

"Locating and tracking a cell-site simulator," Beckwith wrote, "has the substantial potential to expose the owner's intimate personal information," particularly their movements and whereabouts. "A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will."

For that reason, Beckwith said, “the use of a cell-site simulator to locate Mr. Jones’s phone invaded a reasonable expectation of privacy and was thus a search.”

Prosecutors argued that everyone knows that the location of a cellphone can be tracked, and at oral argument one noted that every fleeing criminal on television dramas throws away or destroys their phone. Beckwith disregarded that approach, saying that “a person does not lose a reasonable expectation of privacy merely because he or she is made aware of the government’s capacity to invade his or her privacy.”

Associate Judge Phyllis D. Thompson dissented, though she wrote that under ordinary circumstances, she agreed that the government’s use of a StingRay “likely violates the legitimate expectation of privacy.” But Thompson said Jones forfeited that privacy when he drove around with the victims’ stolen cellphones. Beckwith responded that Jones had not been charged or convicted of stealing the phones at the time of the search.

The StingRay issue is separate from another cellphone issue pending before the Supreme Court — whether law enforcement must obtain a warrant before obtaining a cellphone’s historical location data from a phone company. Phone companies record which cell towers are used when a call is made, which police often use to demonstrate a person’s whereabouts at the time of a crime. Those records can be obtained with a court order, and a lower standard of proof, rather than a warrant. The ACLU’s Wessler said that Thursday’s ruling was a “recognition that constitutional protections must keep pace with advancing technology, and is an important reminder of what is at stake as the Supreme Court takes up the issue of police requests for historical cellphone location data.”

From: (b)(6); (b)(7)(C)
Sent: 22 Sep 2017 12:32:33 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) (Desk)
202-839-(b)(7) (Cell)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:06 PM

To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5)

Sent with BlackBerry Work (www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Sep 22, 2017, 10:41 AM
To: (b)(6); (b)(7)(C),
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); are asking.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6);
202-538-(b)(7)(C) (iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:43 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)

(b)(6);
CLS, HSILD, OPLA, ICE
202-732(b)(6);
202-538(b)(7)(C) (iPhone)

From (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:38 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

Police use of 'StingRay' cellphone tracker requires search warrant, appeals court rules

By Tom Jackman September 21 at 5:20 PM
<< OLE Object: Picture (Device Independent Bitmap) >>
A "StingRay II," made by the Harris Corp., can redirect cellphone calls away from cell tower

antennae and capture their identifying data and location. Police use them to find people. Some argue that that's an invasion of privacy. (Courtesy Harris Corp.)

A device that tricks cellphones into sending it their location information and has been used quietly by policeand federal agents for years, requires a search warrant before it is turned on, an appeals court in Washington ruled Thursday. It is the fourth such ruling by either a state appeals court or federal district court, and may end up deciding the issue unless the government takes the case to the U.S. Supreme Court or persuades the city's highest court to reverse the ruling.

The case against Prince Jones in 2013 involved D.C. police use of a "StingRay" cell-site simulator, which enables law enforcement to pinpoint the location of a cellphone more precisely than a phone company can when triangulating a signal between cell towers or using a phone's GPS function. Civil liberties advocates say the StingRay, by providing someone's location to police without court approval, is a violation of an individual's Fourth Amendment right not to be unreasonably searched. The D.C. Court of Appeals agreed in a 2 to 1 ruling, echoing similar rulings in the Maryland Court of Special Appeals and federal district courts in New York City and San Francisco.

"This opinion," said Nathan F. Wessler of the American Civil Liberties Union, who helped argue the case with the D.C. Public Defender Service, "joins the growing chorus of courts holding that the Fourth Amendment protects against warrantless use of invasive, covert technology to track people's phones. … We applaud today's opinion for erecting sensible and strong protections against the government violating people's privacy in the digital age."

The U.S. attorney's office in Washington declined to comment on the ruling. The prosecutors could ask for a rehearing by the three judge panel or the entire appeals court, and if those are denied take the case to the Supreme Court, though Wessler noted that the high court might not be inclined to take a case where there is no dispute among the lower court rulings.

The Justice Department issued policy guidance to its agencies in 2015 that a search warrant must be obtained for all StingRay uses, and though that is not binding on state and local police, the Metropolitan Police Department has said it would abide by that rule. The ACLU has counted 72 cell-site simulators in use in 24 states and the District, but believes there could be many more. Both D.C. and Baltimore police had signed an agreement with the FBI not to disclose or discuss their StingRay device publicly, court records show, and an FBI agent sat with prosecutors during Jones's trial to advise them on how to handle questions about the device.

The ruling by the D.C. Court of Appeals resulted in all the evidence in the case against Jones being thrown out, and a nine-count felony conviction for sexual abuse, kidnapping, armed robbery and threats being vacated.

Jones was arrested after he allegedly assaulted and robbed two women in separate incidents, after arranging to meet with them through Backpage.com for sexual liaisons. In both cases, the perpetrator took the victims' cellphones.

After the second incident, D.C. police compared the call records of the victims and found that the same phone number had been used to arrange both meetings. The police then obtained the mobile identification number for the man's phone, as well as the identification numbers for the victims' phones, and with the help of the phone companies obtained a general location for the phones, which police said appeared to be traveling together.

Once in the vicinity of the phones, the police turned on the StingRay, court records show, and punched in the identification number (different from the phone number) of the assailant's phone. The StingRay acts like a cell site antenna, and convinces cellphones to connect to it instead of a real cell site, providing the phone numbers and locations of the phones that connect. The phones are useless during this time because they aren't connected to an actual network, only the StingRay.

Before long, the assailant's prepaid cellphone was found on Jones, sitting in a parked car on Minnesota Avenue in Northeast Washington, as were the phones stolen from the victims, police said. The appeals court ruled, and the defense agreed, that if the police had used the StingRay on one of the victims' phones, instead of Jones's phone, the search would have been legal because the victims consented to the search.

The judge in Jones's trial declined to suppress the phone seizure, which in turn led to the knife apparently used in the robberies, the discovery of the victims' phones and incriminating statements made by Jones and his girlfriend. But the ruling written by Associate Judge Corinne A. Beckwith, joined by Senior Judge Michael W. Farrell, threw out all of that evidence as "fruit of the poisonous tree," namely the StingRay.

"Locating and tracking a cell-site simulator," Beckwith wrote, "has the substantial potential to expose the owner's intimate personal information," particularly their movements and whereabouts. "A cell-site simulator allows police officers who possess a person's telephone number to discover that person's precise location remotely and at will."

For that reason, Beckwith said, "the use of a cell-site simulator to locate Mr. Jones's phone invaded a reasonable expectation of privacy and was thus a search."

Prosecutors argued that everyone knows that the location of a cellphone can be tracked, and at oral argument one noted that every fleeing criminal on television dramas throws away or destroys their phone. Beckwith disregarded that approach, saying that "a person does not lose a reasonable expectation of privacy merely because he or she is made aware of the government's capacity to invade his or her privacy."

Associate Judge Phyllis D. Thompson dissented, though she wrote that under ordinary circumstances, she agreed that the government's use of a StingRay "likely violates the legitimate expectation of privacy." But Thompson said Jones forfeited that privacy when he drove around

with the victims' stolen cellphones. Beckwith responded that Jones had not been charged or convicted of stealing the phones at the time of the search.

The StingRay issue is separate from another cellphone issue pending before the Supreme Court — whether law enforcement must obtain a warrant before obtaining a cellphone's historical location data from a phone company. Phone companies record which cell towers are used when a call is made, which police often use to demonstrate a person's whereabouts at the time of a crime. Those records can be obtained with a court order, and a lower standard of proof, rather than a warrant. The ACLU's Wessler said that Thursday's ruling was a "recognition that constitutional protections must keep pace with advancing technology, and is an important reminder of what is at stake as the Supreme Court takes up the issue of police requests for historical cellphone location data."

From: (b)(6); (b)(7)(C)
Sent: 22 Sep 2017 12:06:09 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5)

Sent with BlackBerry Work (www.blackberry.com)

From: (b)(6); (b)(7)(C) >
Date: Friday, Sep 22, 2017, 10:41 AM
To: (b)(6); (b)(7)(C)
<(b)(6); (b)(7)(C)
<
Cc: (b)(6); (b)(7)(C)
<(b)(6); (b)(7)(C) >
Subject: RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(C) are asking.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C)
202-538- iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:43 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C)
202-538-(iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:38 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

Police use of 'StingRay' cellphone tracker requires search

From: (b)(6); (b)(7)(C)
Sent: 22 Sep 2017 11:52:54 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

I've asked (b)(6); (b)(7)(to look into, but if you can ask tech Ops, that would be great.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6);
202-538-(b)(7)(Phone)
C)

***** Warning *** Attorney/Client Privilege *** Attorney Work Product *****
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 11:47 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

I had no visibility on this case. I'll reach out to Tech Ops to see if they heard of it.

Sent with BlackBerry Work (www.blackberry.com)

From: (b)(6); (b)(7)(C)>
Date: Friday, Sep 22, 2017, 10:41 AM
To: (b)(6); (b)(7)(C)>,
(b)(6); (b)(7)(C)>
Cc: (b)(6); (b)(7)(C)>
Subject: RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(are asking.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6);
202-538-(b)(7)((iPhone)
C)

***** Warning *** Attorney/Client Privilege *** Attorney Work Product *****
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:43 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-
202-538- (b)(6); (b)(7)(C) iPhone)

***** Warning *** Attorney/Client Privilege *** Attorney Work Product *****
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:38 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: New Adverse on Cell Site Simulators?

From: (b)(6); (b)(7)(C)
Sent: 22 Sep 2017 11:47:08 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

I had no visibility on this case. I'll reach out to Tech Ops to see if they heard of it.

Sent with BlackBerry Work (www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Sep 22, 2017, 10:41 AM
To (b)(6); (b)(7)(C)
<(b)(6); (b)(7)(C)
<
Cc: (b)(6); (b)(7)(C)
<(b)(6); (b)(7)(C)
Subject: RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(are asking.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732
202-538 (b)(6); (b)(7)(C) (iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:43 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6);
202-538-(b)(7)(C) (iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:38 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

Police use of 'StingRay' cellphone tracker requires search

From: (b)(6); (b)(7)(C)
Sent: 22 Sep 2017 13:10:37 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

Thanks again.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C)
202-538-(iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 1:09 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

1) Not HSI.
2) DC Metropolitan Police Department (MPD).
3) *Jones v. United States*, No. 15-CF-322 (D.C. Cir. Sept. 21, 2017) *[strange citation since not case not yet published in a reporter]*

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-3832 (Desk)
202-839-1672 (Cell)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:42 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

Hit send too soon. Two questions:

1) This was not an HSI case, right? What agency was it?

2) Can you please send me the cite?

I know. That's three questions. But I only had two numbers so back off. Thanks.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6);
202-538-(b)(7)(C) (iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:40 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

Thank you both.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6)
202-538-(b)(7) (iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:33 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); Desk)
202-839-(b)(7)(C) Cell)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 12:06 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: New Adverse on Cell Site Simulators?

(b)(5)

Sent with BlackBerry Work (www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Sep 22, 2017, 10:41 AM
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: New Adverse on Cell Site Simulators?

Anyone? The (b)(6); (b)(7)(are asking.

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732
202-538 (b)(6); (b)(7)(C) Phone)

Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From: Liberta, Joseph M
Sent: Friday, September 22, 2017 9:43 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C)
202-538- (iPhone)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 22, 2017 9:38 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: New Adverse on Cell Site Simulators?

Did you folks see this one yet? Do we need to formulate/update guidance for our clients to keep them on the right side of the law here?

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 18:58:10 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: query - CLS SME re Cell Site Simulator

Thanks, I spoke w (b)(6) and am getting more info on it – I forwarded them the DHS policy and spoke w/ (b)(6); at Tech Ops who provided (b)(6); as the POC in (b)(7)(E) that they are already working with it appears) for the practical aspects / access to the technology, itself, language for pen / R41 warrant, etc. I'll keep you posted – if you know of that case out of NY let me know.

(b)(6);

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 2:53 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: query - CLS SME re Cell Site Simulator

(b)(6);
There may be a case out of NY on point for this fact pattern. We can discuss on Monday if it's not urgent.

(b)(6);

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 11:35 AM
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)>
Cc: (b)(6); (b)(7)(C)>,
(b)(6); (b)(7)(C)>
Subject: RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks, (b)(6);

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 11:17 AM
To: OPLA-CLS; (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Thanks (b)(6); (b)(7)(C) you're the only one on the team here today so can you get in touch with (b)(6);

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (b)(7)(C) (Desk)
202-536-(b)(6); (b)(7)(C) (Cell)

From: OPLA-CLS (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 11:11 AM
To: (b)(6); (b)(7)(C)
Cc:
(b)(6); (b)(7)(C)
Subject: FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); to the CLS inbox seeking guidance on the use of cell cite simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

(b)(6);

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) (office)
202-494-[redacted] (mobile)
(b)(6); (b)(7)(C)

From (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 10:41 AM
To: OPLA-CLS
Subject: query - CLS SME re Cell Site Simulator

CLS Colleagues:

(b)(5); (b)(7)(E)

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you,

(b)(6);
(b)(6);
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6 (w)
202-904- (c)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 14:53:13 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: query - CLS SME re Cell Site Simulator

(b)(6);

There may be a case out of NY on point for this fact pattern. We can discuss on Monday if it's not urgent.

(b)(6);
(b)(7)(C)

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 11:35 AM
To: (b)(6); (b)(7)(C), (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C), (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks, (b)(6);

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 11:17 AM
To: OPLA-CLS; (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Thanks, (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6);

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (Desk)
202-536-(b)(7)(C) (Cell)

*** Warning *** Attorney/Client Privilege *** Attorney Work Product ***
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement

sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From: OPLA-CLS <(b)(6); (b)(7)(C) >
Date: Friday, Jun 09, 2017, 11:11 AM
To: (b)(6); (b)(7)(C)
<(b)(6); (b)(7)(C) >
Cc: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); to the CLS inbox seeking guidance on the use of cell cite simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); office)
202-494-(b)(7) mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 10:41 AM
To: OPLA-CLS
Subject: query - CLS SME re Cell Site Simulator

CLS Colleagues:

(b)(5); (b)(7)(E)

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you,

(b)(6);
(b)(7)(C)
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) w)
202-904- c)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 11:17:13 -0400
To: OPLA-CLS (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Thanks, (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6)

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (Desk)
202-536-(b)(7) (Cell)

From: OPLA-CLS <(b)(6); (b)(7)(C)>
Date: Friday, Jun 09, 2017, 11:11 AM
To: (b)(6); (b)(7)(C)
<(b)(6); (b)(7)(C)>
Cc: (b)(6); (b)(7)(C)
<(b)(6); (b)(7)(C)
Subject: FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); to the CLS inbox seeking guidance on the use of cell cite simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

(b)(6);

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) (office)
202-494- (mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 10:41 AM
To: OPLA-CLS
Subject: query - CLS SME re Cell Site Simulator

CLS Colleagues:

(b)(5); (b)(7)(E)

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you,

(b)(6);
(b)(7)(C)
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6 w)
202-904-b. c)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 15:35:27 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks, (b)(6);

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 11:17 AM
To: OPLA-CLS; (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Thanks, (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6); (b)(7)(

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732 (b)(6); (Desk)
202-536 (b)(7)(C) (Cell)

From: OPLA-CLS <(b)(6); (b)(7)(C)>
Date: Friday, Jun 09, 2017, 11:11 AM
To: (b)(6); (b)(7)(C) >
Cc:
(b)(6); (b)(7)(C) >
Subject: FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); (b)(7)(C) to the CLS inbox seeking guidance on the use of cell cite simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

(b)(6);
(b)(7)(C)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-73 (b)(6); (b)(7)((office)
202-49 (mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 10:41 AM
To: OPLA-CLS
Subject: query - CLS SME re Cell Site Simulator

CLS Colleagues:

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you (b)(6);

(b)(6);
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732 (b)(6 (w)
202-904 (c)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 19:04:05 +0000
To: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Where is it, I've been sitting at your desk all day until a few minutes ago.

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 3:01 PM
To: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

If you go into my office, on the desk behind my chair, on the far right side, there is a folder divider with folders in it. One should be labeled cell site, ignore the one labeled (b)(6); (b)(7)(C) In it should be the NY case printed out. If it can wait, I'll find it on Monday.

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 2:58 PM
To: (b)(6); (b)(7)(C), OPLA-CLS <(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Thanks, I spoke w/ (b)(6) and am getting more info on it – I forwarded them the DHS policy and spoke w/ (b)(6); at Tech Ops who provided (b)(6); (b)(7)(C) as the POC in (b)(7)(E) that they are already working with it appears) for the practical aspects / access to the technology, itself, language for pen / R41 warrant, etc. I'll keep you posted – if you know of that case out of NY let me know.

(b)(6);

From (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 2:53 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: query - CLS SME re Cell Site Simulator

(b)(6);
There may be a case out of NY on point for this fact pattern. We can discuss on Monday if it's not urgent.

(b)(6);

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 11:35 AM
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C),
(b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks (b)(6);

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 11:17 AM
To: OPLA-CLS; (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Thanks, (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6)

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); Desk)
202-536-(b)(7)(C) Cell)

From: OPLA-CLS <(b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 11:11 AM
To: (b)(6); (b)(7)(C)
Cc:
(b)(6); (b)(7)(C)
Subject: FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); to the CLS inbox seeking guidance on the use of cell cite simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

(b)(6);

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732 (b)(6); (b)(7)(office)
202-494 mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 10:41 AM
To: OPLA-CLS
Subject: query - CLS SME re Cell Site Simulator

CLS Colleagues:

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 14:53:13 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: query - CLS SME re Cell Site Simulator

(b)(6);

There may be a case out of NY on point for this fact pattern. We can discuss on Monday if it's not urgent.

(b)(6);
(b)(7)(C)

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 11:35 AM
To: (b)(6); (b)(7)(C),
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks, (b)(6);

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 11:17 AM
To: OPLA-CLS; (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Thanks (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6);

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732 (b)(6); (Desk)
202-536 (b)(7)(C) (Cell)

From: OPLA-CLS <(b)(6); (b)(7)(C)>
Date: Friday, Jun 09, 2017, 11:11 AM
To: (b)(6); (b)(7)(C)
<(b)(6); (b)(7)(C)>
Cc: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: FW: query - CLS SME re Cell Site Simulator

Good Morning,

Please note the email below from (b)(6); to the CLS inbox seeking guidance on the use of cell cite simulator technology. Recommend someone from Tech Ops team provide assistance.

Best,

(b)(6);

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (office)
202-494-(b)(7); (mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 10:41 AM
To: OPLA-CLS
Subject: query - CLS SME re Cell Site Simulator

CLS Colleagues:

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you, (b)(6);

(b)(6);
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) w)
202-904- c)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 15:00:48 -0400
To: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

If you go into my office, on the desk behind my chair, on the far right side, there is a folder divider with folders in it. One should be labeled cell site, ignore the one labeled (b)(6); (b)(7)(C) In it should be the NY case printed out. If it can wait, I'll find it on Monday.

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 2:58 PM
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Thanks, I spoke w/ (b)(6) and am getting more info on it – I forwarded them the DHS policy and spoke w/ (b)(6); at Tech Ops who provided (b)(6); (b)(7)(C) as the POC in (b)(7)(E) (that they are already working with it appears) for the practical aspects / access to the technology, itself, language for pen / R41 warrant, etc. I'll keep you posted – if you know of that case out of NY let me know.

(b)(6);

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 2:53 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: query - CLS SME re Cell Site Simulator

(b)(6);
There may be a case out of NY on point for this fact pattern. We can discuss on Monday if it's not urgent.

(b)(6);

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 11:35 AM

To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Yes, I will. Thanks, (b)(6);

From: (b)(6); (b)(7)(C)
Sent: Friday, June 09, 2017 11:17 AM
To: OPLA-CLS; (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: query - CLS SME re Cell Site Simulator

Thanks, (b)(6); (b)(7)(C) - you're the only one on the team here today so can you get in touch with (b)(6 ?

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); Desk)
202-536-(b)(7)(Cell)

From: OPLA-CLS <(b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 11:11 AM
To: (b)(6); (b)(7)(C)
<(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: FW: query - CLS SME re Cell Site Simulator

Good Morning,

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 13:34:39 -0400
To: (b)(6); (b)(7)(C)
Subject: RE: question on Stingrays

Is about 20 min ok?

(b)(6); (b)(7)(C)
Homeland Security Investigations
National Program Manager
Technical Enforcement Officer
703-551-(b)(6) Desk
571-839-[illegible] Mobile
(b)(6); (b)(7)(C)

Technical Support: ICE Service Desk: (888) 347-(b)(6);
VECADS Support: VECADS 24/7 Support Desk: (888) 4VE(b)(6); 1-888-483-(b)(6); or
(b)(6); (b)(7)(C)
CVN Support: Spectrum Support Desk: (703) 551-(b)(6); or
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 1:33 PM
To: (b)(6); (b)(7)(C)
Subject: question on Stingrays

(b)(6);

(b)(6); (b)(7)(C) thought you might be able to assist – I have an inquiry through our embed in (b)(7)(E) about current practices involving cell-site simulators – do you have time for a call?

Thanks, (b)(6);

(b)(6); (b)(7)(C)

Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
(202) 732-(b)(6) (office)
(202) 308- (cell)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 17:31:00 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: (b)(6); (b)(7)(C) and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); (b)(7)(C) Tracking Warrant + (b)(7)(E) decision)

(b)(6); (b)(7)(C) -

Many thanks for the guidance and all the supporting information in this message. It definetely will lend itself to a productive discussion with ERO Leadership. I believe this gives us the necessary ammunition to tackle this head-on. This is a marquee case for us, and we are extremely grateful for your counsel.

I'll be in touch with further developments as they surface.

Regards,

(b)(6); (b)(7)(C)
ICE-ERO-TLEO
Deputy Assistant Director
Global Police Services Division
USNCB-INTERPOL Washington
Mobile: 202-697-(b)(6);

From: (b)(6); (b)(7)(C) >
Date: Friday, Jun 09, 2017, 4:38 PM
To: (b)(6); (b)(7)(C)
Cc: >
Subject: (b)(6); and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); (b)(7)(C) Tracking Warrant + (b)(7)(E) Cir. decision)

(b)(6); –

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(6);
(b)(7)(C)
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6)w)
202-904-[illegible]c)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 9 Jun 2017 18:15:44 -0400
To: (b)(6); (b)(7)(C)
Subject: RE: (b)(6); and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); Tracking Warrant + (b)(7)(Cir. decision)

(b)(6);
Thanks so much for your generosity, advice, and time today. I really appreciate it. Have a wonderful weekend.

(b)(6);
202-904(b)(6); c

From: (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 5:31 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: (b)(6); and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); Tracking Warrant + (b)(7)(E) Cir. decision)

(b)(6);
(b)(7)(C) -

Many thanks for the guidance and all the supporting information in this message. It definetely will lend itself to a productive discussion with ERO Leadership. I believe this gives us the necessary ammunition to tackle this head-on. This is a marquee case for us, and we are extremely grateful for your counsel.

I'll be in touch with further developments as they surface.

Regards,

(b)(6); (b)(7)(C)
ICE-ERO-TLEO
Deputy Assistant Director
Global Police Services Division
USNCB-INTERPOL Washington

Mobile: 202-697-(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Date: Friday, Jun 09, 2017, 4:38 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: (b)(6); (b)(7)(C) and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); (b)(7)(C) Tracking Warrant + (b)(7)(C) Cir. decision)

(b)(6); (b)(7)(C) –

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(6);
(b)(7)(C)
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 17 Nov 2017 10:46:53 -0500
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: RE: News: If NYPD cops want to snoop on your phone, they need a warrant, judge rules

Wait – what? (See my highlights, below.)

And what the heck are you reading???

(b)(6); (b)(7)(C)
Chief
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C)
202-538- iPhone)

From: (b)(6);
Sent: Friday, November 17, 2017 10:33 AM
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: News: If NYPD cops want to snoop on your phone, they need a warrant, judge rules

Just a state trial court decision, but thought it was noteworthy.

---

https://arstechnica.com/tech-policy/2017/11/if-nypd-cops-want-to-snoop-on-your-phone-they-need-a-warrant-judge-rules/

If NYPD cops want to snoop on your phone, they need a warrant, judge rules

NY State Supreme Court: Stingrays act as "an instrument of eavesdropping."

CYRUS FARIVAR - 11/17/2017, 5:03 AM

A New York state judge has concluded that a powerful police surveillance tool known as a stingray, a device that spoofs legitimate mobile phone towers, performs a "search" and therefore requires a warrant under most circumstances.

As a New York State Supreme Court judge in Brooklyn ruled earlier this month in an attempted murder case, New York Police Department officers should have sought a standard, probable cause-driven warrant before using the invasive device.

The Empire State court joins others nationwide in reaching this conclusion. In September, the District of Columbia Court of Appeals also found that stingrays normally require a warrant, as did a federal judge in Oakland, California, back in August.

According to *The New York Times*, which first reported the case on Wednesday, *People v. Gordon* is believed to be the first stingray-related case connected to the country's largest city police force.

"By its very nature, then, the use of a cell site simulator intrudes upon an individual's reasonable expectation of privacy, acting as an instrument of eavesdropping and requires a separate warrant supported by probable cause rather than a mere *pen register/trap and trace* order such as the one obtained in this case by the *NYPD,"* Justice Martin Murphy wrote in the November 3 decision.

A "pen register" warrant, sometimes known as a "pen/trap order," which typically only provides a call log for a particular number, has been used in the era of stingrays to also include location information. Historically, law enforcement officers nationwide have not been forthright with judges when explaining what the devices do.

(b)(5)

(b)(5)

In this case, the suspect, Shuquan Gordon, was located in a Brooklyn apartment building seemingly out of nowhere. This was "an address not previously identified as of any interest to this investigation," as the judge noted.

Brian Owsley, a law professor at the University of North Texas and a former federal magistrate judge, whose 2014 law review article on stingrays was cited numerous times by the Brooklyn judge, told Ars that this ruling fell in line with what he called "positive momentum" toward proper regulation.

"There is still a long way to go," he e-mailed. "Moreover, as good as this decision is, the current progress is more aptly described as two steps forward followed by one step back."

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) office)
202-731-; mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 3 Aug 2017 15:09:29 -0400
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: Noteworthy tech news

Thanks (b)(6); This bitcoin issue just came up on an AFU call about whether this impacts our current forfeiture procedures.

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (Desk)
202-536-(b)(7)(C) (Cell)

From: (b)(6);
Sent: Wednesday, August 2, 2017 1:54 PM
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: Noteworthy tech news

Sharing with Cyber, Tech Ops, and Financial.

8. TR Daily– **"Four Senators Press DOJ on Cell-Site Simulator Disclosures"** – Four senators wrote AG Sessions today to urge DOJ to inform judges about the impacts of cell-site simulators such as Stingrays on 911 calls and other communications of Americans.

11. Ars Technica– **"Why the Bitcoin network just split in half and why it matters"** – The confusing result is that if you owned one bitcoin before the split you own two bitcoins now: one coin on

the original Bitcoin network, and a second coin on the new Bitcoin Cash network. The two coins have the same cryptographic credentials, but they have very different values if you sell them for old-fashioned dollars. Long read.

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section|Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) (desk)
202-731- (mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 27 Jul 2017 13:16:39 +0000
To: (b)(6); (b)(7)(C)
Subject: Cell-site simulator canvassing warrant go-by 2015 09 10.docx
Attachments: Cell-site simulator canvassing warrant go-by 2015 09 10.docx

Here you go.. let me know if you need anything else.

WARRANT FOR THE USE OF A CELL-SITE SIMULATOR TO OBTAIN IDENTIFIERS OF A CELL PHONE OR OTHER CELLULAR DEVICE AT PARTICULAR LOCATIONS ("CANVASSING")

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

IN THE UNITED STATES DISTRICT COURT
FOR _____

IN THE MATTER OF THE USE OF A CELL-SITE SIMULATOR TO IDENTITY THE CELLULAR DEVICE CARRIED BY [[SUSPECT]]	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

ATTACHMENT A

(b)(5)

ATTACHMENT B

(b)(5)

From: (b)(6); (b)(7)(C)
Sent: 30 Aug 2016 14:16:03 +0000
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: State v. Andrews
Attachments: andrews-maryland_court_of_special_appeals_opinion.pdf

[Sending to Tech Ops, Cyber and Cyber Forensics and cc'ing all CLS]

Attached is a Md Ct. of Appeals Dec., *State v. Andrews*, on cell-site simulators. From the Homeland Sec. Inst. conference (b)(6) and I attended last week (and just generally) this is a hot topic; expect there to be more litigation. This case is fairly recent – 3/16.

(b)(5); (b)(6); (b)(7)(C)

Very general breakdown (of course); just FYI,

(b)(6); (b)(7)(C)
Associate Legal Advisor
U.S. Immigration and Customs Enforcement
Office of the Principal Legal Advisor
Homeland Security Investigations Law Division
Criminal Law Section
(202) 732-(b)(6) (office)
(202) 308-(b)(7) (iPhone)
(b)(6); (b)(7)(C)

REPORTED

IN THE COURT OF SPECIAL APPEALS

OF MARYLAND

No. 1496

September Term, 2015

STATE OF MARYLAND

v.

KERRON ANDREWS

Leahy,
Friedman,
Thieme, Raymond G., Jr.
(Retired, Specially Assigned)

JJ.

Opinion by Leahy, J.

Filed: March 30, 2016

> "[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."

Riley v. California, 134 S. Ct. 2473, 2484 (2014).

This case presents a Fourth Amendment issue of first impression in this State: whether a cell phone—a piece of technology so ubiquitous as to be on the person of practically every citizen—may be transformed into a real-time tracking device by the government without a warrant.

On the evening of May 5, 2014, the Baltimore City Police Department (BPD) used an active cell site simulator, without a warrant, to locate Appellee Kerron Andrews who was wanted on charges of attempted murder. The cell site simulator, known under the brand name "Hailstorm," forced Andrews's cell phone into transmitting signals that allowed the police to track it to a precise location inside a residence located at 5032 Clifton Avenue in Baltimore City. The officers found Andrews sitting on the couch in the living room and arrested him pursuant to a valid arrest warrant. The cell phone was in his pants pocket. After obtaining a warrant to search the residence, the police found a gun in the cushions of the couch.

In the Circuit Court for Baltimore City, Andrews successfully argued that the warrantless use of the Hailstorm device was an unreasonable search under the Fourth Amendment of the United States Constitution. The court suppressed all evidence obtained by the police from the residence as fruit of the poisonous tree. The State, pursuant to Maryland Code (1973, 2013 Repl. Vol., 2015 Supp.), Courts and Judicial Proceedings Article ("CJP"), § 12-302(c)(4), now appeals the court's decision to suppress that evidence.

The specific questions before us, as framed by the State, are:

1) Did the motions court err in finding that the use of a cellular tracking device to locate Andrews's phone violated the Fourth Amendment?

2) Did the motions court err in finding that Andrews did not have to show standing before challenging the search of the home where he was arrested?

3) Did the motions court err in finding that the search warrant for the home where Andrews was located was invalid?

4) Did the motions court err in excluding the items recovered in this case?

We conclude that people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement, and—recognizing that the Fourth Amendment protects people and not simply areas—that people have an objectively reasonable expectation of privacy in real-time cell phone location information. Thus, we hold that the use of a cell site simulator requires a valid search warrant, or an order satisfying the constitutional requisites of a warrant, unless an established exception to the warrant requirement applies.

We hold that BPD's use of Hailstorm was not supported by a warrant or an order requiring a showing of probable cause and reasonable limitations on the scope and manner of the search. Once the constitutionally tainted information, obtained through the use of Hailstorm, was excised from the subsequently issued search warrant for 5032 Clifton Avenue, what remained was insufficient to establish probable cause for a search of that residence. Because the antecedent Fourth Amendment violation by police provided the only information relied upon to establish probable cause in their warrant application, those

same officers cannot find shelter in the good faith exception, and the evidence seized in that search withers as fruit of the poisoned tree. We affirm.

BACKGROUND

Andrews was positively identified via photographic array as the person who shot three people on April 27, 2014, as they were attempting to purchase drugs on the 4900 block of Stafford Street in Baltimore City.[1] He was charged with attempted first-degree murder and attendant offenses in connection with the shooting, and a warrant for his arrest was issued on May 2, 2014.

Pen Register and Trap & Trace Order

Unable to locate Andrews, Detective Michael Spinnato of the BPD confirmed Andrews's cell phone number through a confidential informant, and then submitted an application in the Circuit Court for Baltimore City for a pen register/trap & trace order for Andrews's cell phone.[2] Specifically, Det. Spinnato requested authorization for the

---

[1] The State later admitted that there were also two negative photo arrays.

[2] As discussed further *infra*, pursuant to the Maryland Pen Register, Trap and Trace Statute, found at CJP § 10-4B-01 *et seq.* ("Maryland pen register statute"), a court having jurisdiction over the crime being investigated may authorize the use of a "pen register" and/or a "trap and trace device," defined as:

> 'Pen register' means a device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.

CJP § 10-4B-01(c)(1). The statute continues, stating:

> 'Trap and trace device' means a device or process that captures the incoming electronic or other impulses that identify the originating number or other

"installation and use of device known as a "Pen Register\Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits, which registers telephone numbers dialed or pulsed from or to the telephone(s) having the number(s) . . . ." The application stated that Andrews was aware of the arrest warrant, and that to hide from police

> suspects will contact family, girlfriends, and other acquaintances to assist in their day to day covert affairs. Detective Spinnato would like to track/monitor Mr. Andrews'[s] cell phone activity to further the investigation an [sic] assist in Mr. Andrews'[s] apprehension.
>
> * * *
>
> Your Applicant hereby certifies that the information likely to be obtained concerning the aforesaid individual's location will be obtained by learning the numbers, locations and subscribers of the telephone number(s) being dialed or pulsed from or to the aforesaid telephone and that such information is relevant to the ongoing criminal investigation being conducted by the Agency.

On May 5, 2014, Det. Spinnato's application was approved in a signed order stating, in part:

> **[T]he Court finds that probable cause exists and that the applicant has certified that the information likely to be obtained by the use of the above listed device(s) is relevant to an ongoing criminal investigation,** To wit: Attempted Murder.
>
> * * *

(Emphasis in original). And, as requested in the application, the court,

---

> dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.

CJP § 10-4B-01(d)(1). Under Maryland law, an order for a pen register/trap & trace is issued without a warrant and on something less than probable cause.

> **ORDERED,** pursuant to Section 10-4B-04 of the Courts and Judicial Proceedings Article . . . [Applicants] are authorized to use for a period of sixty (60) days from the date of installation, a Pen Register \ Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits . . .
>
> * * *
>
> **ORDERED,** . . . [t]he Agencies are *authorized to employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of a Pen Register \ Trap & Trace and Cellular Tracking Device*, unobtrusively and with a minimum of interference to the service of subscriber(s) of the aforesaid telephone, and *shall initiate a signal to determine the location of the subject's mobile device . . . .*

(Emphasis added).

Cell Phone in a Hailstorm

As soon as Det. Spinnato obtained the pen register\trap & trace order on May 5, he sent a copy to the BPD's Advanced Technical Team (the "ATT"). The ATT then issued a form request to the service provider (Sprint) for the following: subscriber information; historical cell site location information ("CSLI") for the period from April 5 to May 5, 2014; pen register data for 60 days; and precision GPS data from Andrews's phone.[3] An additional request followed for "GPS Precise Locations and email."

[3] Two broad categories of CSLI may be sought from the service provider. The first is historical CSLI, which is used to look back through service provider records to determine a suspect's location at a given point in the past. *See, e.g.*, *United States v. Graham*, 796 F.3d 332, 343 (4th Cir. 2015) ("Historical CSLI identifies cell sites, or 'base stations,' to and from which a cell phone has sent or received radio signals, and the particular points in time at which these transmissions occurred, over a given timeframe. . . . The cell sites listed can be used to interpolate the path the cell phone, and the person carrying the phone, travelled during a given time period."), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015). Law enforcement frequently uses historical CSLI to prove that a defendant was in the area where a crime of which he is accused occurred. The second category of CSLI is real-time data, used to track the whereabouts and movements of a suspect by using the cell

Later on the same day—May 5—Det. Spinnato began receiving emails from ATT with GPS coordinates for Andrews's cell phone (within a range of a 200 to 1600 meter radius). Det. Spinnato and officers from the Warrant Apprehension Task Force ("WATF") proceeded to the general area and waited until they received information from ATT that the cell phone was in the area of 5000 Clifton Avenue, Baltimore City. They proceeded to an area where there were approximately 30 to 35 apartments around a U-shaped sidewalk. Detective John Haley from ATT arrived and, using a cell site simulator known by the brand name "Hailstorm," was able to pinpoint the location of the cell phone as being inside the residence at 5032 Clifton Avenue.[4]

Det. Spinnato knocked on the door and, after obtaining the consent of the woman who answered, entered the residence along with several other officers. They found Andrews seated on the couch in the living room with the cell phone in his pants pocket.

---

phone as a tracking device. *See, e.g.*, *Tracey v. State*, 152 So. 3d 504, 507 (Fla. 2014), *reh'g denied* (Dec. 8, 2014). Here, the BPD obtained real-time location information from the service provider when it received the GPS coordinates associated with the cell phone from Sprint. Andrews's motion to suppress, however, was focused primarily on the BPD's ensuing use of a cell site simulator to directly obtain pin-point location data. Therefore, on appeal we do not address whether the real-time location information from Sprint should have been obtained under a warrant or special order.

[4] True to its brand name, the Hailstorm device generates an electronic barrage that impacts all the mobile devices within its range. As noted in the *amicus* brief filed by the American Civil Liberties Union ("ACLU") and Electronic Frontier Foundation ("EFF") at page 3, the fact that cell site simulators actively locate phones by forcing them to repeatedly transmit their unique identifying electronic serial numbers, and then calculating the signal strength until the target phone is pinpointed, is found in several recent federal publications and cases, including a Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology 2 (Sept. 3, 2015), *available at* https://www.justice.gov/opa/file/767321/download [https://perma.cc/K99L-H643].

Det. Spinnato arrested Andrews and secured the location until a search warrant could be obtained. Once they had the warrant, the BPD searched the home and found a gun in the couch cushions.

Initial Hearings

Andrews was indicted by a grand jury on May 29, 2014, on numerous charges related to the April 27, 2014 shooting. On July 1, 2014, the Assistant Public Defender representing Andrews filed an "omnibus" motion including requests for discovery and the production of documents. The State responded with an initial disclosure and supplemental disclosure on July 9 and 11, respectively. Those disclosures, however, failed to reveal the method used to locate Andrews on the date of his arrest.

On November 3, 2014, defense counsel filed a supplemental discovery request seeking, *inter alia*, "[a]ll evidence indicating how Andrews was located at 5032 Clifton Avenue." The State's response to that request, dated January 8, 2015, stated, "[a]t this time the State does not possess information related to the method used to locate [Andrews] at 5032 Clifton Avenue." However, five months later defense counsel received an email from the Assistant State's Attorney ("ASA") assigned to the case indicating that it was her understanding that "the ATT used a stingray to locate[] your client via his cell phone," but she was waiting for "the paperwork." The next day, May 7, the ASA also notified defense counsel of exculpatory evidence in the form of a negative photo array that was conducted the previous January.

On May 12, 2015, defense counsel requested that the court dismiss the case based on discovery violations and moved for suppression of evidence, including the gun, phone

records, and identification testimony. A few days later, on May 15, the State filed a supplemental disclosure, which provided:

> WATF did not have the Clifton Ave address as a possible location until ATT provided that information. Det. Spinnato recalls that he was in touch with Det. Haley from ATT. ATT was provided that information from Sprint in the form of GPS coordinates, Det. Spinnato received the same information either from Sprint directly, or forwarded from ATT. Det. Spinnato provided ATT with the phone number associated to Defendant from the shooting investigation and, [redacted in original]-Det. Spinnato recalls that ATT gave Det. Spinnato the Clifton Ave address in the afternoon/early evening on May 5, 2014. . . .

The State's supplemental disclosure also identified a second negative photo array conducted on May 4, 2014.

Andrews's initial motions were heard in the circuit court on May 12, 21, and June 4, 2015. At the conclusion of the hearing on June 4, the circuit court found that one of the lead investigators intentionally withheld exculpatory evidence—including both negative photo arrays. As a result, the circuit court partially granted the pending defense motion for sanctions and excluded that detective's testimony from trial. The court declined to dismiss the case and denied the motion to exclude the gun and cell phone on the basis of the State's withholding of discoverable materials. However, as a consequence of the State's failure to timely disclose information concerning Hailstorm surveillance technology that was used by the BPD, the Court granted the defense additional time to file a motion to suppress.

Motion to Suppress

Andrews filed a Motion to Suppress—over 50 pages including exhibits—on June 30, 2015, in which he challenged the BPD's surreptitious use of the Hailstorm cell site simulator to search Andrews's phone, without a warrant, under the Fourth Amendment to

the United States Constitution. Andrews moved to suppress all evidence obtained from 5032 Clifton Avenue.

During the ensuing hearing on the motion to suppress, held August 20, 2015, the State suggested, and the defense agreed, that the circuit court rely on the transcripts and exhibits from the earlier motions hearings for an understanding of the function of the Hailstorm device and its use by the BPD:

> [STATE'S ATTORNEY]: . . . The exact testimony that we're going to hear about with regard to the Fourth Amendment issue Counsel heard as it related to the discovery issue because the discovery issue bled into the Fourth Amendment issue. So there is nothing new. There is nothing -- Counsel's aware that the equipment is called Hailstorm not Stingray because of the testimony that Counsel heard and extracted from the detective as it relates to this very case. So there simply is, there is nothing new. We're at the exact same issue that we were two months ago.
>
> THE COURT: So do we even need, do you need to call the witness or can I just rely on the transcript?
>
> [STATE'S ATTORNEY]: It would seem to me to rely on the transcript.
>
> * * *
>
> THE COURT: . . . So the State is indicating that the testimony that the State would present today is the same testimony that was presented --
>
> [DEFENSE COUNSEL]: Right.
>
> THE COURT: -- there.
>
> [DEFENSE COUNSEL]: Right.
>
> THE COURT: And that's in the transcript, and the Court can just rely on the transcript to rule on your motion.
>
> [DEFENSE COUNSEL]: Right.
>
> THE COURT: You're fine with that?

[DEFENSE COUNSEL]: Yep.

The court took a recess for several hours to review the motions and transcripts. The following excerpts from the June 4th hearing, entered as Defendant's Exhibit 1C, pertain to the function of the cell site simulator:

> [DETECTIVE HALEY]: What happened in this case was, Detective Sp[innato] from our WATF, which is the Warrant Apprehension Unit, apparently interviewed somebody -- got a phone number. He then responds down here to the Circuit Court . . . and gets a Court Order signed.
>
> He then sends the Court order down to our office, depending on what the carrier is, Verizon, Sprint, T-Mobile, AT&T. We then send it to them. I ask for subscriber information, call-detail records.
>
> They provide us with GPS locations, in this case. And once we get all the information, then we have equipment that we can go out and locate cell phones.
>
> [DEFENSE COUNSEL]: Okay. When you say, we have equipment that we can locate cell phones, you're talking about the Stingray equipment, is that what was used in this case?
>
> [DETECTIVE HALEY]: Yeah, it's called the Hailstorm. It used to be -- Stingray is kind of first generation.
>
> * * *
>
> [DEFENSE COUNSEL]: Tell me what the Hailstorm does.
>
> [DETECTIVE HALEY]: What we get from the phone company is the subscriber information. So, when we get the subscriber information, it has a [sic] identifier on there, if you will, a serial number. We put that into the Hailstorm equipment. And the Hailstorm equipment acts like a cell tower. So, we go into a certain area, and basically, the equipment is looking for that particular identifier, that serial number.
>
> [DEFENSE COUNSEL]: Okay. And so, if a person is inside of a home, that equipment peers over the wall of the home, to see if that cell phone is behind the wall of that house, right?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: And it sends an electronic transmission through the wall of that house, correct?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: Did you get a separate search warrant for that search into the home?

[DETECTIVE HALEY]: You'd have to talk to Detective Spinnato about that. Because he's the one that got the Court Order signed.

[DEFENSE COUNSEL]: Did you do the search? You conducted the equipment in this -- you operated –

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: -- the equipment?

[DETECTIVE HALEY]: Yes.

* * *

[DEFENSE COUNSEL]: Tell me all of the information the Hailstorm can retrieve from a phone.

[DETECTIVE HALEY]: It's going to retrieve, like I said before, the serial number of the phone, depending on what kind of phone it is. It's going to -- there's [sic] different identifiers. Like for Sprint, in this case, it's called the MSID. And that's like a ten-digit -- like a ten-digit number. So, it's retrieving that. And there's also the electronic serial number. It's retrieving that. And that's really it.

[DEFENSE COUNSEL]: Can you capture the telephone calls as they're being made?

[DETECTIVE HALEY]: No.

[DEFENSE COUNSEL]: And how do you know where the phone -- and it doesn't capture any data on the phone?

[DETECTIVE HALEY]: No.

[DEFENSE COUNSEL]: Are you sure?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: So, how do you get information about where the phone is on the machine?

[DETECTIVE HALEY]: Because when it captures that identifier that you put into the machine or the equipment, it then tells you -- it looks like a clock on the equipment. And it tells you where the signal's coming from, like 12, 1, 2, 3 o'clock (indicating). And it will give you like a reading. Like if it says 1:00 at like an 80, well, then you know that you're kind of close to it. But if it says 1:00 at like a 40, then you know that you're probably within, I don't know, probably, you know, 20 yards of it.

[DEFENSE COUNSEL]: The person doesn't have to be using their phone for you to get that information, do they?

[DETECTIVE HALEY]: Actually, if they're on their phone, then they're already connected to -- in this case, the Sprint network. And we're not going to be able to pull them off of that until they're -- until they hang -- until they hang the call up.

[DEFENSE COUNSEL]: So, they hang the call up. And the phone can be in their pocket, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: And then you're reaching in to grab an electronic signal about where that phone is? It's not pinging, in other words, right?

* * *

MR. HALEY: Like I said, our equipment acts like a cell tower. So, it draws the phone to our equipment.

[DEFENSE COUNSEL]: But you just said, if the person's on the phone, your equipment won't work, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: So, it doesn't act like a cell tower, because you can find the phone only when they are not on the phone, correct?

[DETECTIVE HALEY]: Well, I would say it does act like a cell tower, because the only time that you're going to connect -- the only time that you're going to connect to the network, or to a tower is when you go to try to use it.

[DEFENSE COUNSEL]: But you're connecting to where the phone is, when they're not on the phone, didn't you just say that

[DETECTIVE HALEY]: Maybe I'm getting confused, or I'm not understanding what you're asking me.

[DEFENSE COUNSEL]: My question to you was, for example, I have my phone in my pocket. And I'm sitting in my house, right?

[DETECTIVE HALEY]: Okay.

[DEFENSE COUNSEL]: And you want to know where I am, correct?

[DETECTIVE HALEY]: Okay.

* * *

[DEFENSE COUNSEL]: When I am not on my phone, you will drive by my house, and you will get a signal from my phone indicating where I am, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: If I am using the phone, you won't get that signal, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: So, the phone cannot be in use. You are searching for my phone as you're driving through my neighborhood, right?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: And in order to get to my phone, you are sending an electronic signal into my house, right?

[DETECTIVE HALEY]: Yes.

When the hearing resumed, the court made several preliminary findings, and invited counsel to respond. In regard to the pen register/trap & trace order, the court observed:

> I don't find that Judge Williams' order is invalid as a pen register or trap and trace, but I do find that the order does not authorize the use of Hailstorm and I . . . invite the State to tell me otherwise.
>
> * * *
>
> So this is very different from an order authorizing, for example, GPS or cell site information, because that is information that's generated by the phone. And my understanding of this equipment is essentially that it's forcing the phone to emit information, or its taking information from the phone that the phone is not sort of on its own generating at the time which is very different.

On the issue of whether Andrews's arrest was lawful, the parties acknowledged that a valid warrant was outstanding for his arrest. However, the court questioned whether, as argued by defense counsel, Andrews's presence at 5032 Clifton Avenue "or the warrant they got as a result of him being there is fruit of the poisonous tree because there was a violation of his Fourth Amendment rights by [Det. Haley] using the Hailstorm on this phone to locate him at that residence in the first place." Looking then to the application for the warrant to search 5032 Clifton Avenue, the court noted that there was no independent corroboration for the warrant because, "all it says he was located at this address and so we want to search this address. I mean that's really all it says."

After hearing argument, the circuit court found that "the use of the Hailstorm violates the Defendant's Fourth Amendment rights," and "any information generated from the use of the Hailstorm [must] be suppressed." The court continued on the record:

> And so just so that I'm clear, it means that the jury cannot hear any testimony or evidence about information obtained from the Hailstorm, obtained through the Hailstorm device. And just so that I'm clear, it's my

understanding that the Hailstorm device is what told the police that the Defendant was at that location.

And so that includes any testimony or evidence then that the Defendant was at that location, if that's what -- because that's what the Hailstorm told the police. And so the jury would be prohibited from hearing evidence or testimony of that. It does not invalidate the arrest or the search [incident to] the arrest with the phone that's in his pocket.[5]

Now anything that came off the phone, again if it came through the Hailstorm device it is suppressed. There can be no evidence or testimony about it. And then again, any police knowledge that the Defendant was at that location again also suppressed, so the jury would not be able to hear any evidence or testimony of that.

So then that leaves us with the fruit of the poisonous tree argument for the search and seizure warrant. I reviewed the warrant and it literally says the Defendant was in there so now we need a warrant. And information generated from the use of the Hailstorm be suppressed, that's all that it is. And so I analyze this different, a little bit different from a normal sort of motion to suppress a search and seizure warrant or even *Franks* in terms of standing.

I don't -- I understand the State's argument in terms of standing and this not being his residence, and the Defense's argument that he was at a minimum an overnight guest and has some reasonable expectation of privacy. I don't think I need to reach those issues because the warrant is really just fruit of the poisonous tree of the illegally obtained information about the Defendant's location. That's what it is.

And so I am granting the suppression of that for that very reason. And so that the record is clear – and I know that the State is asking to take an appeal, the record is clear. The ruling of the Court is that the government violated the Defendant's Fourth Amendment rights by essentially using the Hailstorm to locate him at that residence.

The State noticed its appeal on September 3, 2015.

---

[5] Mr. Andrews did not challenge the legality of his arrest or search incident to arrest, either in the circuit court or before this Court. He did, however, seek to suppress the cell phone, but that motion was denied and Mr. Andrews did not file a cross-appeal to contest that ruling.

DISCUSSION

Motion to Dismiss

Before turning to the merits, we must address Andrews's motion to dismiss this appeal on the ground that the notice of appeal was defective, and therefore, not filed within the time prescribed by Rule 8-202.

The State filed its notice of appeal on September 3, 2015; however, the signed certificate of service—indicating that a copy of the notice was "mailed first-class, postage prepaid" on that same day—failed to list the party that was served. Andrews acknowledges that a copy of the notice was delivered to the Office of the Public Defender on September 4, 2015. Nevertheless, Andrews argues that the State's notice did not comply with the certificate of service requirements of Maryland Rule 1-323, and that the clerk should not have accepted the filing. Consequently, according to Andrews, no valid notice of appeal was filed in this case. The State concedes that the failure to name the party to be served was a defect in the certificate of service, but maintains the clerk was required to accept the filing because the certificate complied with the literal requirements of Rule 1-323. The State urges that it would be improper to dismiss the appeal because there is no dispute that the opposing party was served in a timely fashion.

Maryland Rule 1-323 directs that the court clerk may not accept for filing a pleading or other paper requiring service, unless it is accompanied by "an admission or waiver of service or a signed certificate showing the date and manner of making service." In *Director of Finance of Baltimore City v. Harris*, this Court addressed whether a certificate of service that failed to identify all the persons upon whom service was required should have been

rejected for filing by the court clerk. 90 Md. App. 506, 513-14 (1992). Looking to the 1984 revision of the Maryland Rules that produced the current Rule 1-323, this Court observed:

> Under the old Rule, the clerk may have had some obligation to determine whether the certificate actually showed service on the "opposite party." But, as noted, that obligation, if it ever did exist, has been eliminated. . . . The obligation of the clerk under the current Rule is simply to assure that there is, in fact, an admission, a waiver, or a certificate showing the date and manner of service. If such a certificate is attached to the paper, the clerk must file the paper, leaving it then to the parties or the court to deal with any deficiency.[6]

More recently, in *Lovero v. Da Silva*, this Court clarified that, by mandating that proof of service (or a waiver of service) appear on each pleading or paper, "Rule 1-323 assures the court . . . that each party has been duly notified before action is taken by the court in response to or as a result of the subject pleading or paper." 200 Md. App. 433,

---

[6] This Court further illuminated the evolution of Rule 1-323 stating:

> Rule 1-323 is derived ultimately from Rule 1(a)(2), Part Two, V, of the General Rules of Practice and Procedure, adopted by the Court of Appeals and approved by the General Assembly pursuant to 1939 Md. Laws, ch. 719, § 35A. Rule 1(a)(2) provided, in relevant part, that a paper "shall not be received and filed by the clerk of the court unless accompanied by an admission or proof of service of a copy thereof *upon the opposite party or his attorney of record* in accordance with this rule." (Emphasis added.) Other parts of the Rule prescribed how service was to be made. That Rule was carried over into the Maryland Rules of Procedure as Rule 306 a.2., which stated that "[t]he clerk shall not accept or file any paper requiring service other than an original pleading unless it is accompanied by an admission or proof of service of a copy thereof *upon the opposite party, or his attorney of record.*" (Emphasis added.)
>
> Until the 1984 revision of the Maryland Rules, the Rule remained in that form.

Harris, 90 Md. App. at 511-12.

446 (2011). We determined that Lovero's notice of appeal should have been rejected by the clerk, explaining that

> [w]here, as in the instant case, the notice of appeal contains no proof of service whatsoever, we have no basis upon which to conclude that the notice of appeal was served on the opposing party or parties. Indeed, it is undisputed here that the Notice of Appeal was never served on Da Silva.

Id. at 449.

In the present case, there is no dispute that the notice was served on defense counsel. Indeed, the State made it clear at the August 20 hearing that it would be filing an appeal as reflected in the court's ruling; "and so that the record is clear – and I know that the State is asking to take an appeal, the record is clear." It is also clear now that, although the omission in the certificate of service is a defect, the certificate met the literal requirements of Rule 1-323—it provided the date and manner of service. Where there is no evidence that Andrews was prejudiced or that the course of the appeal was delayed by a defect, "it is the practice of this Court to decide appeals on the merits rather than on technicalities." *Bond v. Slavin*, 157 Md. App. 340, 352-53 (2004). *Cf. Williams v. Hofmann Balancing Techniques, Ltd.*, 139 Md. App. 339, 356-57 (2001) (holding that the appellant's failure to identify one of the appellees on his notice of appeal did not deprive this Court of jurisdiction). To be sure, the Court of Appeals has observed that "[o]ur cases, and those of the Court of Special Appeals, have generally been quite liberal in construing timely orders for appeal." *Newman v. Reilly*, 314 Md. 364, 386 (1988); *see also Lovero*, 200 Md. App. at 450-51 n.8 (and the cases cited therein) (recognizing that where a challenged notice of

appeal was timely filed the courts of Maryland construe the notice in favor of deciding the appeal on the merits). We deny Andrews's motion to dismiss the appeal.

Standard of Review

We review the grant of a motion to suppress based on the record of the suppression hearing, and we view the facts in the light most favorable to the prevailing party. *State v. Donaldson*, 221 Md. App. 134, 138 (citing *Holt v. State,* 435 Md. 443, 457, 78 A.3d 415 (2013)), *cert. denied,* 442 Md. 745 (2015). Further, "we extend 'great deference' to the factual findings and credibility determinations of the circuit court, and review those findings only for clear error." *Id.* (citing *Brown v. State,* 397 Md. 89, 98 (2007)). But we make an independent, *de novo*, appraisal of whether a constitutional right has been violated by applying the law to facts presented in a particular case. *Williams v. State,* 372 Md. 386, 401 (2002) (citations omitted); *see also Brown*, 397 Md. at 98 ("[W]e review the court's legal conclusions *de novo* and exercise our independent judgment as to whether an officer's encounter with a criminal defendant was lawful." (Citation omitted)).

I.

Fourth Amendment Search

In 1966, in the wake of prominent Congressional hearings on government invasions of privacy, Justice Douglas, dissenting in *Osborn v. United States* and *Lewis v. United States*, and concurring in *Hoffa v. United States*, observed:

> We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. The aggressive breaches of privacy by the Government increase by geometric proportions. Wiretapping and 'bugging' run rampant, without effective judicial or legislative control.

* * *

> Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of man's life at will.

Osborn v. United States, 385 U.S. 323, 340-43 (1966) (Douglas, J., dissenting).[7] Fifty years later we face the same concern—to what extent have advances in technology created an "age of no privacy."[8]

The Fourth Amendment to the United States Constitution, made applicable to the States by the Fourteenth Amendment, *Mapp v. Ohio*, 367 U.S. 643, 655 (1961), provides:

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

U.S. Const. amend. IV. The first clause protects individuals against unreasonable searches and seizures,[9] *see Katz v. United States*, 389 U.S. 347, 359 (1967) ("Wherever a man may

---

[7] The question presented in *Osborn*, as cast by Justice Douglas, was "whether the Government may compound the invasion of privacy by using hidden recording devices to record incriminating statements made by the unwary suspect to a secret federal agent." *Osborn*, 385 U.S. at 340.

[8] *See also City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

[9] Although the parties do not present their arguments under the Maryland Constitution, Declaration of Rights, we note that Article 26—governing warrants for search and seizure—is generally construed to be co-extensive with the Fourth Amendment. *See Upshur v. State*, 208 Md. App. 383, 397 (2012) (citing *Hamel v. State,* 179 Md. App. 1, 18 (2008)). Article 26 of the Maryland Declaration of Rights provides:

be, he is entitled to know that he will remain free from unreasonable searches and seizures[]"), and the second clause requires that warrants must be particular and supported by probable cause, *see Payton v. New York*, 445 U.S. 573, 584 (1980).

A "search" within the meaning of the Fourth Amendment occurs where the government invades a matter in which a person has an expectation of privacy that society is willing to recognize as reasonable. *Kyllo v. United States,* 533 U.S. 27, 33 (2001) (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)). As we made clear in *Raynor v. State*, "[t]he burden of demonstrating a 'legitimate' or 'reasonable' expectation of privacy includes both a subjective and an objective component." 201 Md. App. 209, 218 (2011), *aff'd*, 440 Md. 71 (2014) (citation and footnote omitted). "[I]n order to claim the protection of the Fourth Amendment, a defendant must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable; *i.e.*, one that has 'a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.'" *Minnesota v. Carter,* 525 U.S. 83, 88 (1998) (quoting *Rakas v. Illinois,* 439 U.S. 128, 143-44 n.12 (1978)).

> That all warrants, without oath or affirmation, to search suspected places, or to seize any person or property, are grievous and oppressive; and all general warrants to search suspected places, or to apprehend suspected persons, without naming or describing the place, or the person in special, are illegal, and ought not to be granted.

The Fourth Amendment protects not against all intrusions as such, "but **against intrusions which are not justified in the circumstances, or which are made in an improper manner**." *Maryland v. King*, 133 S. Ct. 1958, 1969 (2013) (emphasis added) (quoting *Schmerber v. California*, 384 U.S. 757, 768 (1966)). "Although the underlying command of the Fourth Amendment is always that searches and seizures be reasonable, *what is reasonable depends on the context within which a search takes place.*" *State v. Alexander,* 124 Md. App. 258, 265 (1998) (emphasis added in *Alexander*) (quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985)). Subject to a few well-delineated exceptions, "warrantless searches 'are *per se* unreasonable under the Fourth Amendment.'" *Quon*, 560 U.S. at 760 (2010) (quoting *Katz*, 389 U.S. at 357); *see also United States v. Karo*, 468 U.S. 705, 717 (1984) (citations omitted).

a. Effects of the Nondisclosure Agreement

Before we examine the reasonableness of the State's intrusion *in context*, we address the nondisclosure agreement entered into between the State's Attorney for Baltimore City and the Federal Bureau of Investigation in early August 2011 as a condition of BPD's purchase of certain "wireless collection equipment/technology manufactured by Harris [Corporation]." The nondisclosure agreement provided, in part:

> [T]o ensure that [] wireless collection equipment/technology continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and **use shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including b[ut] not limited to: in press release, in court documents, during judicial hearings**, or during other public forums or proceedings. Accordingly, the Baltimore City Police Department agrees to the following

> conditions in connection with its purchase and use of the Harris Corporation equipment/technology:
>
> * * *
>
> 5. The Baltimore City Police Department and Office of the State's Attorney for Baltimore City **shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use the equipment/technology including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State's case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI**. . . .

(Emphasis added). The agreement directs that in the event of a Freedom of Information Act request, or a court order directing disclosure of information regarding Harris Corporation equipment or technology, the FBI must be notified immediately to allow them time to intervene "and potential[ly] compromise." If necessary "the Office of the State's Attorney for Baltimore will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to provide, any information concerning the Harris Corporation wireless collection equipment/technology[.]"

We observe that such an extensive prohibition on disclosure of information to the court—from special order and/or warrant application through appellate review—prevents the court from exercising its fundamental duties under the Constitution. To undertake the Fourth Amendment analysis and ascertain "the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security," *Terry v. Ohio*, 392

U.S. 1, 19 (1968), it is self-evident that the court must understand why and *how* the search is to be conducted. The reasonableness of a search or seizure depends "'on a **balance** between the public interest and the individual's right to personal security free from arbitrary interference by law officers.'" *Pennsylvania v. Mimms*, 434 U.S. 106, 109 (1977) (emphasis added) (quoting *United States v. Brignoni-Ponce*, 422 U.S. 873, 878 (1975)). The analytical framework requires analysis of the functionality of the surveillance device and the range of information potentially revealed by its use. A nondisclosure agreement that prevents law enforcement from providing details sufficient to assure the court that a novel method of conducting a search is a reasonable intrusion made in a proper manner and "justified by the circumstances," obstructs the court's ability to make the necessary constitutional appraisal. *Cf. King*, 133 S. Ct. at 1970 ("Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution. Urgent government interests are not a license for indiscriminate police behavior."). In *West v. State*, this Court stated that "to assure that the purpose of the Fourth Amendment is upheld, police officers must provide details within affidavits when attempting to acquire search warrants, even if such information would seem to the police officer of trivial consequence at the time." 137 Md. App. 314, 331 (2001).

As discussed further in Section III *infra*, it appears that as a consequence of the nondisclosure agreement, rather than apply for a warrant, prosecutors and police obtained an order under the Maryland pen register statute that failed to provide the necessary information upon which the court could make the constitutional assessments mandated in this case. The BPD certified to the court that pursuant to the order "the information likely

to be obtained concerning the aforesaid individual's location will be obtained by learning the numbers, locations and subscribers of the **telephone number(s) being dialed or pulsed from or to the aforesaid telephone** . . . ." However, the suppression court, having the benefit of Det. Haley's testimony (reproduced above), learned that the BPD actually employed the Hailstorm device, which is capable of obtaining active real-time location information—far different from a pen register (a device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument) or track and trace device (a device or process that captures the incoming electronic or other impulses that identify the originating number). *See* fn.2 *supra*.[10]

We perceive the State's actions in this case to protect the Hailstorm technology, driven by a nondisclosure agreement to which it bound itself, as detrimental to its position and inimical to the constitutional principles we revere.

b. What Constitutes a "Search"—Level of Intrusion and Expectation of Privacy

The State argues that the use of a cell site simulator does not constitute a "search" under the Fourth Amendment. The State maintains that the circuit court's decision "was based upon both factually unreasonable conclusions about how the cell site simulator worked in this case, and legally incorrect determinations about what constitutes a 'search.'" The State acknowledges that the factual bases for the circuit court's rulings are found in the June 4, 2015 testimony of Det. Haley. However, the State argues that Det. Haley's

[10] It is not clear from the record whether Det. Haley's testimony was authorized through written approval from the FBI as required in paragraph 5 of the nondisclosure agreement.

testimony "was necessarily rather summary," and does not support the factual conclusions of the circuit court.

According to the State, the cell site simulator "acts like a cell tower, and waits to receive a signal bearing the target IMSI" [International Mobil Subscriber Identity]. The State maintains that, properly construed, Det. Haley's testimony reveals that "the process of a cell phone sending its identifying information to a cell tower was indistinguishable from the process of a cell phone sending its identifying information to a cell site simulator." The State asserts that the Hailstorm device "merely reads the ID number regularly transmitted by activated cell phones as part of their ordinary use" and "[w]hen the device detects a signal from the target phone, it notifies the operator the direction of the signal and the relative strength, allowing the operator to estimate the probable location of the phone." Therefore, the State argues that no reasonable expectation of privacy existed in the information obtained by the Hailstorm device and no intrusion or "search" occurred.

Andrews countercharges that there was ample, explicit support in the record for the circuit court's finding that the Hailstorm device operated by emitting a signal "through the wall of a house" and "into the phone" triggering the phone to respond to the device. Andrews argues that, through the use of an "active cellular surveillance device," the State violated his reasonable expectation of privacy in the personal information contained and generated by his cell phone, without which the government would not have been able to discover his location inside the home.

Presumably because of the nondisclosure agreement discussed above, the State provided limited information regarding the function and use of the Hailstorm device. And

presumably, the State would have limited itself in this manner regardless of whether it relied on testimony from the prior hearing or produced live testimony before the suppression court.[11] Notwithstanding this, it is clear from Det. Haley's testimony that "the Hailstorm equipment acts like a cell tower," but, unlike a cell tower awaiting incoming signals, the Hailstorm is an active device that can send an electronic signal through the wall of a house and "draw[] the phone to [the] equipment." Based on the direction and strength of the signal the Hailstorm receives from a cell phone in response, law enforcement can pinpoint the real-time location of a cell phone (and likely the person to whom it belongs) within less than 20 yards.

These points from Det. Haley's testimony regarding the function of the Hailstorm device are consistent with what other courts and legal scholars have been able to discern about the device. Hailstorm, along with the earlier-model cell site simulator known as "StingRay," to which Det. Haley referred, are far from discrete, limited surveillance tools. Rather, as described in a recent article in the Harvard Journal of Law and Technology cited by Appellee and the *amici*:[12]

> This technology, commonly called the StingRay, the most well-known brand name of a family of surveillance devices known more generically as "IMSI

---

[11] In a suppression hearing, "[w]here . . . the defendant establishes initially that the police proceeded warrantlessly, the burden shifts to the State to establish that strong justification existed for proceeding under one of the 'jealously and carefully drawn' exceptions to the warrant requirement." *Jones v. State*, 139 Md. App. 212, 226 (2001) (citation omitted). Where the evidence presented is inconclusive, the consequence for the State is that the defendant wins. *Id.*

[12] In addition to the ACLU and EFF, Professor David Gray of the University of Maryland Francis King Carey School of Law filed a detailed and informative amicus brief in this case.

> catchers," is used by law enforcement agencies to obtain, directly and in real time, unique device identifiers and detailed location information of cellular phones—data that it would otherwise be unable to obtain without the assistance of a wireless carrier.
>
> * * *
>
> By impersonating a cellular network base station, a StingRay—a surveillance device that can be carried by hand, installed in a vehicle, or even mounted on a drone—**tricks all nearby phones and other mobile devices into identifying themselves (by revealing their unique serial numbers)** just as they would register with genuine base stations in the immediate vicinity. As each phone in the area identifies itself, the StingRay can determine the location from which the signal came.

Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J. L. & Tech. 134, 142, 145-46 (2014) (emphasis added; footnotes omitted).

The Supreme Court of Wisconsin examined whether law enforcement could obtain location data through cell site information or a StingRay pursuant to a warrant and, before holding that the warrant was sufficiently particularized, based on probable cause, and passed constitutional muster, observed:

> A stingray is an electronic device that mimics the signal from a cellphone tower, which causes the cell phone to send a responding signal. If the stingray is within the cell phone's signal range, the stingray measures signals from the phone, and based on the cell phone's signal strength, the stingray can provide an initial general location of the phone. By collecting the cell phone's signals from several locations, the stingray can develop the location of the phone quite precisely.

State v. Tate, 849 N.W.2d 798, 826 n.8 (Wisc. 2014) (citation omitted), *cert. denied*, 135 S. Ct. 1166 (2015); *see also, e.g.*, *In re Application for Pen Register and Trap/Trace Device*

with Cell Site Location Authority, 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) (defining an earlier-model device, the "Triggerfish," as equipment that "enables law enforcement to gather cell site location information directly, without the assistance of the service provider"). We cannot say that the factual findings of the circuit court, in this case, were erroneous; they are firmly grounded in the testimony before that court, and the State has provided no evidence to the contrary.

In determining then whether a Fourth Amendment "search" occurred, we apply the court's factual findings to the test pronounced in *Katz*, *supra*. Rather than limit the constitutional appraisal to a trespass analysis,[13] the *Katz* test requires a two-fold showing: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" 389 U.S. at 361 (Harlan, J., concurring).[14] Even under the more flexible *Katz* test, however, rapid

---

[13] In *Olmstead v. United States,* the Supreme Court held that the government's use of a wire-tapping device over an extended period of time did not constitute a violation of the Fourth Amendment because the wires were installed in a manner that did not constitute a trespass upon the property of the petitioners. 277 U.S. 438, 464 (1928). Thus, the Court stated that a Fourth Amendment violation would occur where there was a tangible, physical intrusion by the government. *Cf. id.* at 466. *Olmstead* was overruled in part by the Court in *Katz*. 389 U.S. at 353.

[14] Maryland appellate courts have, so far, only addressed the admissibility of historical CSLI obtained from a service provider. *See State v. Payne*, 440 Md. 680, 690-91 (2014) (stating that whether a detective "should have been qualified as an expert before being allowed to engage in the process of identifying the geographic location of the cell towers and the locations themselves depends on understanding just what are cell phone records and what their contents reveal."); *Hall v. State*, 225 Md. App. 72, 91 (2015) (concluding that the State's witness was properly qualified as an expert to testify regarding the mapping of appellant's cell phone data); *Stevenson v. State*, 222 Md. App. 118, 129-30 (determining that a *Frye-Reed* hearing on admissibility of novel scientific evidence and expert scientific testimony was not required for admission of cellular tower "ping"

advancements in technology make ascertaining what constitutes a search under the Fourth Amendment ever more challenging.[15]

Charles Katz was charged with transmitting wagering information by telephone in violation of federal law. *Katz*, 389 U.S. at 348. He objected during his trial to the

---

evidence), *cert. denied*, 443 Md. 737 (2015); *Wilder v. State*, 191 Md. App. 319, 364 (2010) (holding that the admission of CSLI required the qualification of the sponsoring witness as an expert); *Coleman-Fuller v. State*, 192 Md. App. 577, 619 (2010) (same). Maryland courts have not previously addressed CSLI in the context of a Fourth Amendment challenge and have never addressed police use of cell site simulators or obtaining real-time CSLI. Because key factual distinctions in this case involve the function of Hailstorm and the ability of law enforcement to track a cell phone directly and in real time, our own cases provide limited guidance.

[15] *See generally* Renée McDonald Hutchins, *Tied Up In Knotts? GPS Technology and The Fourth Amendment*, 55 UCLA L. Rev. 409 (2007). Professor Hutchins notes that the Supreme Court has developed a differential treatment in its intrusiveness analysis under the Fourth Amendment based on the type of information revealed, explaining:

> When gauging the objective reasonableness of various privacy expectations, the Court has leaned heavily on its assessment of the type of information revealed to segregate challenged surveillance technologies into two rough groups: sense-augmenting surveillance and extrasensory surveillance. Sense augmenting surveillance refers to surveillance that reveals information that could theoretically be attained through one of the five human senses. With regard to this type of surveillance, the Court has tended to find that simple mechanical substitutes for or enhancements of human perception typically trigger no Fourth Amendment concerns in cases in which human perception alone would not have required a warrant.
>
> Extrasensory surveillance, conversely, is that which reveals information otherwise indiscernible to the unaided human senses. The Court has adopted a more privacy-protective view of this form of technologically enhanced police conduct. In fact, the case law suggests that surveillance of this type is largely prohibited in the absence of a warrant.

Id. at 432-33.

government's introduction of evidence collected by FBI agents who overheard and recorded his end of telephone conversations from inside a public telephone booth. *Id*. The agents had placed a recording device on the outside of the phone booth from which Katz placed his calls. *Id*. The government contended on appeal that their surveillance did not constitute a search prohibited by the Fourth Amendment because Katz was in a public location that was not constitutionally protected and because the technique they employed involved no physical penetration of the telephone booth. *Id*. at 352. Writing for the majority, Justice Stewart rejected the formulation of the issues by the parties, premised on whether the telephone booth was a "constitutionally protected area," and instructed that "[t]he Fourth Amendment protects people, not places . . . what [Katz] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id*. at 361 (citations omitted). The Court continued, stating that "once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." *Id*. at 350, 353.

Almost 20 years after establishing in *Katz* that an examination of intrusiveness under the Fourth Amendment is not simply measured by physical invasion, the Supreme Court addressed the constitutionality of the government's surreptitious use of a radio transmitter to track the movements of a container to and inside a private residence. *United States v. Karo*, *supra*, 468 U.S. at 709-10. The physical installation of the transmitter was not at issue; rather, the question before the Court was "whether the monitoring of a beeper in a private residence, not open to visual surveillance, violates the Fourth Amendment

rights of those who have a justifiable interest in the privacy of the residence." *Id.* at 714. Although the Court noted that the monitoring of an electronic device is "less intrusive than a full-scale search," it, nevertheless, reveals information about the interior of the residence that the government "could not have otherwise obtained without a warrant." *Id.* at 715. The Supreme Court stated:

> We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.

Id. at 716 (footnote omitted). Notably, the Court also soundly rejected the government's contention that it should be able to engage in warrantless monitoring of an electronic device inside a private residence "if there is the requisite justification in the facts for believing that a crime is being or will be committed and that monitoring the beeper **wherever it goes** is likely to produce evidence of criminal activity." *Id.* at 717 (emphasis added). The Court recognized limited exceptions to the general rule, such as in the case of exigency, but explained why in its view the government exaggerated the difficulties associated with obtaining a warrant:

> The Government argues that the traditional justifications for the warrant requirement are inapplicable in beeper cases, but to a large extent that argument is based upon the contention, rejected above, that the beeper constitutes only a minuscule intrusion on protected privacy interests. The primary reason for the warrant requirement is to interpose a 'neutral and detached magistrate' between the citizen and 'officer engaged in the often competitive enterprise of ferreting out crime.'

* * *

> The Government contends that it would be impossible to describe the 'place' to be searched, because the location of the place is precisely what is sought to be discovered through the search. [ ] However true that may be, it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested.

Id. at 717-18 (citing *Johnson v. United States*, 333 U.S. 10, 14 (1948)).

In *Kyllo*, *supra*, the Supreme Court considered whether a Fourth Amendment search had occurred when the government used a thermal imaging device to detect infrared radiation inside a home. 533 U.S. at 29-30. Federal agents, suspecting that Danny Kyllo was growing marijuana inside his home, were able to confirm areas of heat coming from high intensity lamps used to grow marijuana plants indoors. *Id*. At the threshold of his analysis, Justice Scalia, writing for the majority, observed:

> It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

Id. at 33-34. The Court then noted that, although the *Katz* test—"whether the individual has an expectation of privacy that society is prepared to recognize as reasonable"—may be difficult to apply to some locations, such as telephone booths and automobiles—the expectation of privacy in the home had "roots deep in the common law." *Id.* at 34.

In support of the use of its thermal imaging technology, the government in *Kyllo* argued that there was no "search" because the device detected "'only heat radiating from the external surface of the house[.]'" *Id.* at 35. The Supreme Court, however, cast aside

this contention as the kind of mechanical interpretation rejected in *Katz* and stated, "so also a powerful directional microphone picks up only sound emanating from a house—and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house." *Id.* Rather than abandon *Katz* and take such a mechanical approach, the Court sought to adopt a rule "tak[ing] account of more sophisticated [surveillance] systems that are already in use or in development." *Id.* at 35-36 (footnote omitted). Accordingly, the Court held that "[w]here . . . the Government uses a device that is not in general public use, to explore the details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* at 40. Furthermore, the Court repeated the caveat of *Silverman v. United States,* that the "protection of the home has never been tied to the measurement of the quality or quantity of information obtained" for any invasion of the home, "'by even a fraction of an inch' [is] too much." *Id*. at 37 (quoting *Silverman*, 365 U.S. 505, 512 (1961)).

From *Katz* to *Kyllo*, the Supreme Court has firmly held that use of surveillance technology not in general public use to obtain information about the interior of a home, not otherwise available without trespass, is a "search" under the Fourth Amendment. These decisions resolved to protect an "expectation of privacy that society is prepared to recognize as reasonable." After *Kyllo*, however, the question remained whether electronic tracking or surveillance outside the home could constitute a search under the Fourth Amendment.

In *United States v. Jones*, the Supreme Court reviewed the use of a GPS tracking device affixed to the undercarriage of a vehicle to track the movements of the defendant over a period of 28 days. 132 S. Ct. 945, 948 (2012). The Court unanimously affirmed the United States Court of Appeals for the District of Columbia Circuit's holding that the electronic location surveillance over a period of 28 days was a search and that admission of evidence obtained by the warrantless use of the GPS device violated the Fourth Amendment. The Court was unable, however, to reach full agreement as to the basis for its decision. *See id.* at 953 (majority opinion); 954 (Sotomayor, J., concurring); 967 (Alito, J., concurring in the judgment). Justice Scalia's majority opinion found that a search occurred under the traditional, pre-*Katz* "trespass" rationale, but acknowledged that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* at 953 (emphasis in original).

Agreeing with Justice Brennan's concurrence in *Knotts v. United States*, Justice Scalia expounded that "'when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'" *Id*. at 951 (quoting *Knotts*, 460 U.S. 276, 286 (1983)). When law enforcement placed the GPS tracking system on Jones's vehicle, without a warrant, the government physically invaded a constitutionally protected area, *id.* at 949, 952, and factors beyond trespass need not be considered to find there was a Fourth Amendment violation. *Id*. at 953-54. Justice Scalia explained that the common-law trespass test was essentially a minimum test and that the *Katz* test was "*added to*, not *substituted for*, the common-law trespassory test." *Id.* at 952.

Justice Sotomayor revisited the *Katz* analysis in her concurring opinion, stating that, "even in the absence of a trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'" *Id.* at 954-55 (Sotomayor, J., concurring) (citations omitted). Recognizing that "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance[,]" Justice Sotomayor opined that the unique attributes of GPS location surveillance will require careful application of the *Katz* analysis. *Id.* She urged the Court to update its understanding of peoples' expectations of privacy in the information age:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. *See*, *e.g., People v. Weaver,* 12 N.Y.3d 433, 441–442, 882 N.Y.S.2d 357, 909 N.E.2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. [*United States v.*] *Pineda–Moreno,* 617 F.3d[1120,] 1124 [(9th Cir. 2010)] (opinion of Kozinski, C.J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." *Illinois v. Lidster,* 540 U.S. 419, 426, 124 S.Ct. 885, 157 L.Ed.2d 843 (2004).
>
> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is

> inimical to democratic society." *United States v. Cuevas–Perez,* 640 F.3d 272, 285 (C.A.7 2011) (Flaum, J., concurring).
>
> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques. See *Kyllo,* 533 U.S., at 35, n.2, 121 S.Ct. 2038; *ante,* at 954 (leaving open the possibility that duplicating traditional surveillance "through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy"). I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance," *United States v. Di Re,* 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948).

Jones, 132 S. Ct. at 955-56 (Sotomayor, J., concurring) (footnote omitted).

Justice Alito, concurring only in the judgment, disagreed with the majority's reliance on a trespassory theory. *Jones,* 132 S. Ct. at 958. Instead, Justice Alito found the appropriate inquiry to be "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." *Id.* Justice Alito stated that the majority's reasoning "disregard[ed] what is really important (the *use* of a GPS for the purpose of long-term tracking)" and "will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked." *Id.* at 962 (emphasis in original).

From the above precedent, we glean two broad principles regarding the Fourth Amendment analysis of surveillance technology. First, where surveillance technology is used without a warrant to obtain information about the contents of a home, not otherwise discernable without physical intrusion, there has been an unlawful search. *See Kyllo*, 533 U.S. at 34-35. Second, where the government has engaged in surveillance using "electronic signals without trespass[,]" the intrusion will "*remain* subject to *Katz* analysis." *Jones*, 132 S. Ct. at 953 (emphasis in original). The Supreme Court has recognized, however, that cell phones present novel privacy concerns.

In *Riley*, *supra*, the Supreme Court made clear that a search of the information contained in a cell phone is subject to the warrant requirement regardless of its location. 134 S. Ct. at 2489-91. The Court held that even during a search incident to arrest, the government must first obtain a warrant before searching the digital contents of a cell phone found on the person being arrested. *Id*. at 2485-86.

Chief Justice Roberts described the modern cell phone as much more than a phone:

> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.
>
> One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag

> behind them a trunk of the sort held to require a search warrant in *Chadwick, supra,* rather than a container the size of the cigarette package in *Robinson*.

Id. at 2489.

The State argues that its use of the Hailstorm here should be analogized to *Knotts*, 460 U.S. 276, wherein the Supreme Court upheld law enforcement officers' use of a radio transmitter to track the movements of a container, by automobile, to a defendant's home. In *Knotts*, the Court noted that "[t]he governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways." *Id.* at 281. The Court concluded that:

> A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

Id. at 281-82. Here, the State argues that because Andrews's cell phone was "constantly emitting 'pings' giving its location to the nearest cell tower, . . . there can be no reasonable expectation of privacy in [that] information" under *Knotts*.

The State's reliance on *Knotts*, however, is misplaced. In *Karo*, the Supreme Court clarified that in *Knotts* the electronic device "told the authorities nothing about the interior of Knotts' cabin." 468 U.S. at 715. Rather, the information obtained in *Knotts* was "voluntarily conveyed to anyone who wanted to look[,]" *id.* (quoting *Knotts,* 460 U.S. at 281), and the subsequent search warrant was also supported by "intermittent visual surveillance" of the cabin, *Knotts*, 460 U.S. at 279. As noted in *Kyllo*, the Supreme Court

has long recognized that "[v]isual surveillance [i]s unquestionably lawful because 'the eye cannot by the laws of England be guilty of a trespass.'" 533 U.S. at 31-32 (quoting *Boyd v. United States*, 116 U.S. 616, 628 (1886)).

Here, there was no visual surveillance. The mere fact that police *could* have located Andrews within the residence by following him as he travelled over public thoroughfares does not change the fact that the police did not know where he was, so they could not follow him. Unlike *Knotts*, the information obtained in this case did reveal at least one critical detail about the residence; i.e., that its contents included Andrews's cell phone, and therefore, most likely Andrews himself. Further, "pings" from Andrews's cell phone to the nearest tower were not available "to anyone who wanted to look." We find the surreptitious conversion of a cell phone into a tracking device and the electronic interception of location data from that cell phone markedly distinct from the combined use of visual surveillance and a "beeper to signal the presence of [the defendant's] automobile to the police receiver" to track a vehicle over public roads. *See Knotts*, 460 U.S. at 282. Put simply, the information obtained by police in this case was not readily available and in the public view as it was in *Knotts.*

Cell site simulators, such as Hailstorm, can locate and track the movements of a cell phone and its user across both public and private spaces. Unchecked, the use of this technology would allow the government to discover the private and personal habits of any user. As Justice Sotomayor predicted in her concurring opinion in *Jones*, *supra*, we are compelled to ask "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will,

their political and religious beliefs, sexual habits, and so on." 132 S. Ct. at 956 (Sotomayor, J., concurring). We conclude that they do not.

We agree with the United States Court of Appeals for the Fourth Circuit in *United States v. Graham*, in declaring, "[w]e cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person." 796 F.3d 332, 355 (4th Cir.), *reh'g en banc granted,* 624 F. App'x 75 (4th Cir. 2015).[16] Federal courts reviewing pen register\trap & trace applications have similarly recognized a reasonable expectation of privacy in cell site location information. *See, e.g.*, *In re the Application of the United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006) ("[D]etailed location information, such as triangulation and GPS data, … unquestionably implicate Fourth Amendment privacy rights."); *In re*

[16] The recent cell phone encryption battle between Apple and the United States Government illustrates how fervently people care about protecting their personal location information. In 2011, consumers learned that their iPhones stored months of data regarding Wi-Fi hotspots and cell towers around their location in a format that was not encrypted. The ensuing barrage of complaints caused Apple to revise its operating system to protect consumers' location information. Apple, Inc. Press Release, Apple Q&A on Location Data (April 27, 2011) (available at https://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html) [https://perma.cc/PJ5V-KHGE]. Apple refused to comply with a court order to create software to disable certain security protections of an iPhone. *See* Testimony of Bruce Sewell, *Encryption Tightrope: Balancing American's Security and Privacy*, Hearing before the House Comm. on the Judiciary, 114th Cong. (March 1, 2016); Timothy B. Lee, *Apple's Battle with the FBI over iPhone Security, Explained*, Vox (Feb. 17, 2016), http://www.vox.com/2016/2/17/11037748/fbi-apple-san-bernardino [http://perma.cc/4MFA-JZ4D].

Application of the United States for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed), 402 F. Supp. 2d 597, 604–05 (D. Md. 2005) (recognizing that monitoring of cell phone location information is likely to violate a reasonable expectation of privacy)). We also accept the circuit court's finding in this case that "no one expects that their phone information is being sent directly to the police department on their apparatus."[17] Recognizing that the Fourth Amendment protects people and not simply areas, *Katz*, 389 U.S. at 353, we conclude that people have a reasonable expectation of privacy in real-time cell phone location information.

Moreover, because the use of the cell site simulator in this case revealed the location of the phone and Andrews inside a residence, we are presented with the additional concern that an electronic device not in general public use has been used to obtain information about the contents of a home, not otherwise discernable without physical intrusion. *See Kyllo*, 533 U.S. at 34-35. Under the applicable precedent, this is undoubtedly an intrusion that rises to the level of a Fourth Amendment "search." *See id.* Indeed, "the Fourth Amendment draws a firm line at the entrance to the house[.]" *Id.* at 40 (citation and internal quotation marks omitted). Although we recognize that the use of a cell site simulator to track a phone will not always result in locating the phone within a residence, we agree with the Fourth Circuit's observation that "the government cannot know in advance of obtaining

[17] As the Supreme Court stated in *Katz*, "[t]o read the Constitution more narrowly is to ignore the vital role that the … telephone has come to play in private communication." 389 U.S. at 352.

this information how revealing it will be or whether it will detail the cell phone user's movements in private spaces." *Graham*, 796 F.3d at 350 (citation omitted). The United States District Court for the District of Maryland articulated the same concern when addressing the government's use of a particular cell phone as a tracking device to aid in execution of an arrest warrant. The district court stated:

> Location data from a cell phone is distinguishable from traditional physical surveillance because it enables law enforcement to locate a person entirely divorced from all visual observation. Indeed, this is ostensibly the very characteristic that makes obtaining location data a desirable method of locating the subject of an arrest warrant. This also means, however, that **there is no way to know before receipt of location data whether the phone is physically located in a constitutionally-protected place. In other words, it is impossible for law enforcement agents to determine prior to obtaining real-time location data whether doing so infringes upon the subject's reasonable expectation of privacy and therefore constitutes a Fourth Amendment search.**

In re Application of United States for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 540 (D. Md. 2011) (emphasis added).

It would be impractical to fashion a rule prohibiting a warrantless search only retrospectively based on the fact that the search resulted in locating the cell phone inside a home or some other constitutionally protected area. *See, e.g.*, *Kyllo*, 533 U.S. at 38-39 (declining to adopt a Fourth Amendment standard that would only bar the use of thermal imaging to discern "intimate details" in the home because "no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." (emphasis in original)); *cf.* *Karo*, 468 U.S. at 718 ("We are also unpersuaded by the argument that a warrant should not be required because of the difficulty in satisfying the particularity

requirement of the Fourth Amendment."). Such a rule would provide neither guidance nor deterrence, and would do nothing to thwart unconstitutional intrusions. *Cf. In re the Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device*, 396 F. Supp. 2d 294, 323 (E.D.N.Y.2005) ("Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking . . . which routinely require probable cause." (Internal quotations and citations omitted)).

We determine that cell phone users have an objectively reasonable expectation that their cell phones will not be used as real-time tracking devices through the direct and active interference of law enforcement. We hold, therefore, that the use of a cell site simulator, such as Hailstorm, by the government, requires a search warrant based on probable cause and describing with particularity the object and manner of the search, unless an established exception to the warrant requirement applies.

We turn to consider whether such an exception applies in this case.

c. The Third Party Doctrine

The State maintains that the "Third Party Doctrine" exception to the warrant requirement applied to the BPD's use of Hailstorm to track down Andrews's cell phone. The doctrine—providing that an individual forfeits his or her expectation of privacy in information that is turned over to a third party—finds its strongest expression in *United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979).

In *Smith v. Maryland*, the Supreme Court was presented with the issues of whether the warrantless installation and use of a pen register to collect the telephone numbers dialed from a telephone at the petitioner's home constituted a "search" within the meaning of the Fourth Amendment. 442 U.S. at 736-37. The Court described the function of pen registers, stating that they "'disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purpose of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.'" *Id.* at 741 (quoting *United States v. New York Tel. Co.,* 434 U.S. 159, 167 (1977)). Accordingly, the Court narrowed the issue before it, stating:

> Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.

Id. at 742. In *United States v. Miller*, the Supreme Court held that no reasonable expectation of privacy existed once the owner of financial checks turned financial instruments over to a bank and "exposed [them] to [bank] employees in the ordinary course of business." 425 U.S. at 442.

The State argues that the cell site simulator used in this case merely "detects the signal emitted by the cell phone, just as a regular cell tower would[,]" and, therefore, "the police used data that Andrews voluntarily shared with third parties—specifically his cell phone provider—to locate his phone." The State maintains that, under *Smith* no Fourth Amendment "search" occurred because Andrews had no reasonable expectation of privacy in information he voluntarily transmitted to a third party. The State contends that, by