

227 Md.App. 350  
Court of Special Appeals of Maryland.

STATE of Maryland

v.

Kerron ANDREWS.

No. 1496, Sept. Term, 2015.

|

March 30, 2016.

### Synopsis

**Background:** In prosecution for first-degree murder, the Circuit Court, Baltimore City, [Kendra Ausby, J.](#), granted defendant's motion to suppress. State appealed.

**Holdings:** The Court of Special Appeals, Leahy, J., held that:

[1] as a matter of first impression, defendant had reasonable expectation of privacy in his real-time cell phone location information, and therefore State's use of cell site simulator device was a search subject to Fourth Amendment;

[2] defendant did not voluntarily share his cell site location information with his cell phone provider, and thus, under third party doctrine, defendant did not forfeit his reasonable expectation of privacy in such information;

[3] as a matter of apparent first impression, a pen register trap and trace order is not sufficient to authorize use of cell site simulator; and

[4] as a matter of apparent first impression, pen register trap and trace order obtained by police officers did not operate as the equivalent of a warrant for use of cell site simulator.

Affirmed.

West Headnotes (15)

### [1] Searches and Seizures

#### 🔑 Expectation of privacy

In 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, that is, 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. [U.S.C.A. Const.Amend. 4.](#)

Cases that cite this headnote

### [2] Searches and Seizures

#### 🔑 Persons, Places and Things Protected

#### Searches and Seizures

#### 🔑 Scope, Conduct, and Duration of Warrantless Search

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. [U.S.C.A. Const.Amend. 4.](#)

Cases that cite this headnote

### [3] Searches and Seizures

#### 🔑 Fourth Amendment and reasonableness in general

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. [U.S.C.A. Const.Amend. 4.](#)

Cases that cite this headnote

### [4] Searches and Seizures

#### 🔑 Fourth Amendment and reasonableness in general

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. [U.S.C.A. Const.Amend. 4.](#)

[Cases that cite this headnote](#)

**[5] Searches and Seizures**

🔑 Expectation of privacy

**Telecommunications**

🔑 Carrier's cooperation;pen registers and tracing

Defendant had reasonable expectation of privacy in his real-time cell phone location information, and therefore State's use of cell site simulator device, which sent an electronic signal through wall of house and triggered cell phone to respond, was a search subject to Fourth Amendment; defendant did not volunteer to convey location information simply by choosing to activate and use cell phone and carry device on his person, and information revealed critical detail about house, namely that its contents included defendant's cell phone. [U.S.C.A. Const.Amend. 4.](#)

[3 Cases that cite this headnote](#)

**[6] Searches and Seizures**

🔑 Use of electronic devices;tracking devices or “beepers.”

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. [U.S.C.A. Const.Amend. 4.](#)

[Cases that cite this headnote](#)

**[7] Searches and Seizures**

🔑 Use of electronic devices;tracking devices or “beepers.”

Where the government has engaged in surveillance using electronic signals without trespass, the intrusion will remain subject to *Katz* analysis of whether a Fourth Amendment search has occurred. [U.S.C.A. Const.Amend. 4.](#)

[Cases that cite this headnote](#)

**[8] Searches and Seizures**

🔑 Abandoned, surrendered, or disclaimed items

The “third party doctrine” provides that an individual forfeits his or her expectation of privacy, under the Fourth Amendment, in information that is turned over to a third party. [U.S.C.A. Const.Amend. 4.](#)

[Cases that cite this headnote](#)

**[9] Searches and Seizures**

🔑 Abandoned, surrendered, or disclaimed items

**Telecommunications**

🔑 Carrier's cooperation;pen registers and tracing

Defendant did not voluntarily share his cell site location information with his cell phone provider, and thus, under third party doctrine, defendant did not forfeit his reasonable expectation of privacy in such information, as could obviate warrant requirement for police officers' use of information to locate defendant using cell site simulator; defendant did not engage in any affirmative act such as dialing. [U.S.C.A. Const.Amend. 4.](#)

[2 Cases that cite this headnote](#)

**[10] Searches and Seizures**

🔑 Particular concrete applications

Defendant had standing to challenge search of residence, where use of defendant's real-time cell site location information (CSLI) provided the only support for search of residence, and CSLI was obtained in violation of Fourth Amendment. [U.S.C.A. Const.Amend. 4.](#)

[Cases that cite this headnote](#)

**[11] Criminal Law**

🔑 Presumptions and burden of proof

The burden on a proponent of a motion to suppress is to establish that his own Fourth Amendment rights were violated by

the challenged search or seizure. [U.S.C.A. Const.Amend. 4](#).

[Cases that cite this headnote](#)

## [12] Telecommunications

🔑 Carrier's cooperation;pen registers and tracing

A pen register trap and trace order is not sufficient to authorize use of cell site simulator, which actively sends electronic signal and triggers cell phone to respond. [West's Ann.Md.Code, Courts and Judicial Proceedings, § 10-4B-01](#).

[1 Cases that cite this headnote](#)

## [13] Telecommunications

🔑 Carrier's cooperation;pen registers and tracing

Pen register trap and trace order obtained by police officers did not operate as the equivalent of a warrant, as could allow use of cell site simulator to obtain cell phone location information; limited showing required for trap and trace order fell short of the particularity required for issuance of search warrant, and pen register's reference to "probable cause" merely required that information likely to be obtained was relevant to an ongoing criminal investigation. [U.S.C.A. Const.Amend. 4](#); [West's Ann.Md.Code, Courts and Judicial Proceedings, § 10-4B-01](#).

[2 Cases that cite this headnote](#)

## [14] Searches and Seizures

🔑 Legality of information

No independent lawful source existed to support warrant for search of home, once location information obtained from police officers' unlawful use of cell site simulator was removed, in case in which officers unlawfully used device without a warrant and determined that defendant, for whom an arrest warrant existed, was inside the home; only information linking defendant and home

was the location information from device. [U.S.C.A. Const.Amend. 4](#).

[Cases that cite this headnote](#)

## [15] Criminal Law

🔑 Particular cases

Police officers did not reasonably rely on warrant for search of home, and thus good faith exception to warrant requirement did not apply, in case in which officers illegally used cell site simulator device to determine defendant was inside home, located defendant in the home, and then applied for search warrant for home, where, without the prior unlawful use of cell site simulator device, officers could not have established nexus between alleged criminal activity and home. [U.S.C.A. Const.Amend. 4](#).

[Cases that cite this headnote](#)

## Attorneys and Law Firms

**\*\*326 Robert Taylor, Jr.** (Brian E. Frosh, Atty. Gen., on the brief), Baltimore, for Appellant.

Daniel Kobrin (Paul B. DeWolfe, Public Defender, on the brief), Baltimore, for Appellee.

Panel: LEAHY, FRIEDMAN and RAYMOND G. THIEME, JR. (Retired, Specially Assigned), JJ.

## Opinion

LEAHY, J.

**\*354** “[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*, — U.S. —, 134 S.Ct. 2473, 2484, 189 L.Ed.2d 430 (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.), \*355 [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?

**\*\*327** 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 \*356 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.<sup>1</sup> 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.

<sup>1</sup> The State later admitted that there were also two negative photo arrays.

### 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.<sup>2</sup> Specifically, Det. Spinnato requested authorization for the “installation and use of device known as a “Pen Register \Trap & Trace and Cellular Tracking Device to include cell site information, call detail, \*357 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

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 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.

suspects will contact family, girlfriends, and other acquaintances to assist in \*\*328 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,

**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 \*358 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.<sup>3</sup> An additional request \*\*329 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 Fed.Appx. 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 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.

\*359 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.<sup>4</sup>

<sup>4</sup> 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 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. 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 \*360 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 \*\*330 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.

**\*361** 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.

**\*362** 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.

**\*\*331** 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[inato] 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?

\*363 [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.

\*364 [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 \*\*332 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.

**\*365** [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.

**\*\*333** [DEFENSE COUNSEL]: If I am using the phone, you won't get that signal, right?

**\*366** [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.”

**\*367** 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. <sup>[ 5 ]</sup>

<sup>5</sup> 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.

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 **\*\*334** 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.

**\*368** 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.

## 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 \*369 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, 602 A.2d 191 \(1992\)](#). 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 \*\*335 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.<sup>[ 6 ]</sup>

<sup>6</sup> 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, 602 A.2d 191.

\*370 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, 446, 28 A.3d 43 \(2011\)](#). 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, 28 A.3d 43.

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, 851 A.2d 598 (2004). *Cf.* [Williams v. Hofmann Balancing Techniques, Ltd.](#), 139 Md.App. 339, 356–57, 776 A.2d 4 (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, 550 A.2d 959 (1988); see also *Lovero*, 200 Md.App. at 450–51 n. 8, 28 A.3d 43 (and the cases cited therein) (recognizing that where a challenged notice of appeal was timely filed the courts of Maryland construe \*\*336 the notice in \*371 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, 108 A.3d 500 (citing *Holt v. State*, 435 Md. 443, 457, 78 A.3d 415 (2013)), cert. denied, 442 Md. 745, 114 A.3d 711 (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, 916 A.2d 245 (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, 813 A.2d 231 (2002) (citations omitted); see also *Brown*, 397 Md. at 98, 916 A.2d 245 (“[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 \*372 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, 87 S.Ct. 429, 17 L.Ed.2d 394 (1966) (Douglas, J., dissenting).<sup>7</sup> Fifty years later we face the same concern—to what extent have advances in technology created an “age of no privacy.”<sup>8</sup>

<sup>7</sup> 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, 87 S.Ct. 429.

<sup>8</sup> See also *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760, 130 S.Ct. 2619, 177 L.Ed.2d 216 (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.”).

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, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (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.

\*\*337 U.S. Const. amend. IV. The first clause protects individuals against unreasonable searches and seizures,<sup>9</sup>

see *Katz v. United States*, 389 U.S. 347, 359, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (“Wherever a man may 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, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980).

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, 56 A.3d 620 (2012) (citing *Hamel v. State*, 179 Md.App. 1, 18, 943 A.2d 686 (2008)). Article 26 of the Maryland Declaration of Rights provides:

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.

[1] 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, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (citing *Katz*, 389 U.S. at 361, 88 S.Ct. 507 (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, 29 A.3d 617 (2011), *aff’d*, 440 Md. 71, 99 A.3d 753 (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, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143–44 n. 12, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978)).

[2] [3] 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*, — U.S. —, 133 S.Ct. 1958, 1969, 186 L.Ed.2d 1 (2013) (emphasis added) (quoting *Schmerber v. California*, 384 U.S. 757, 768, 86 S.Ct. 1826, 16 L.Ed.2d 908 (1966)). “Although the underlying command \*374 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, 721 A.2d 275 (1998) (emphasis added in *Alexander*) (quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 337, 105 S.Ct. 733, 83 L.Ed.2d 720 (1985)). Subject to a few well-delineated exceptions, “warrantless searches ‘are *per se* unreasonable under the Fourth Amendment.’” *Quon*, 560 U.S. at 760, 130 S.Ct. 2619 (2010) (quoting *Katz*, 389 U.S. at 357, 88 S.Ct. 507); see also *United States v. Karo*, 468 U.S. 705, 717, 104 S.Ct. 3296, 82 L.Ed.2d 530 (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 \*\*338 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 \*375 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[.]”

[4] 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, 88 S.Ct. 1868, 20 L.Ed.2d 889 (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, 98 S.Ct. 330, 54 L.Ed.2d 331 (1977) (emphasis added) (quoting \*376 *United States v. Brignoni-Ponce*, 422 U.S. 873, 878, 95 S.Ct. 2574, 45 L.Ed.2d 607 (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 \*\*339 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, 768 A.2d 150 (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 \*377 other impulses that identify the originating number). *See* fn.2 *supra*.<sup>10</sup>

<sup>10</sup> 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.

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

[5] 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 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 **\*\*340** 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 **\*378** 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.<sup>11</sup> 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.

<sup>11</sup> 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, 775 A.2d 421 (2001) (citation omitted). Where the evidence presented is inconclusive, the consequence for the State is that the defendant wins. *Id.*

These points from Det. Haley's testimony regarding the function of the Hailstorm device are consistent with what **\*379** 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*:<sup>12</sup>

<sup>12</sup> 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.

This technology, commonly called the StingRay, the most well-known brand name of a family of surveillance devices known more generically as “IMSI 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 **\*\*341** 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 **\*380** 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*, 357 Wis.2d 172, 849 N.W.2d 798, 826 n. 8 (2014) (citation omitted), *cert. denied*, — U.S. —, 135 S.Ct. 1166, 190 L.Ed.2d 921 (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,<sup>13</sup> 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 **\*381** ‘reasonable.’ ” 389 U.S. at 361, 88 S.Ct. 507 (Harlan, J., concurring).<sup>14</sup> Even **\*\*342** under the more flexible *Katz* test, however, rapid advancements in technology make ascertaining what constitutes a search under the Fourth Amendment ever more challenging.<sup>15</sup>

<sup>13</sup> 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, 48 S.Ct. 564, 72 L.Ed. 944 (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, 48 S.Ct. 564. *Olmstead* was overruled in part by the Court in *Katz*. 389 U.S. at 353, 88 S.Ct. 507.

<sup>14</sup> 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, 104 A.3d 142 (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, 123 A.3d 577 (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, 112 A.3d 959 (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” evidence), *cert.*

denied, 443 Md. 737, 118 A.3d 863 (2015); *Wilder v. State*, 191 Md.App. 319, 364, 991 A.2d 172 (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, 995 A.2d 985 (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 Knots? 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.

\*382 Charles Katz was charged with transmitting wagering information by telephone in violation of federal law. *Katz*, 389 U.S. at 348, 88 S.Ct. 507. He objected during his trial to the 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, 88 S.Ct. 507. 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, 88 S.Ct. 507 (citations omitted). The Court continued, stating that “once it is recognized \*\*343 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, 88 S.Ct. 507.

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, 104 S.Ct. 3296. The physical installation of the transmitter was not at issue; rather, the \*383 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, 104 S.Ct. 3296. 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, 104 S.Ct. 3296. 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, 104 S.Ct. 3296 (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, 104 S.Ct. 3296 (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 **\*384** 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.

**\*\*344** *Id.* at 717–18, 104 S.Ct. 3296 (citing *Johnson v. United States*, 333 U.S. 10, 14, 68 S.Ct. 367, 92 L.Ed. 436 (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, 121 S.Ct. 2038. 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, 121 S.Ct. 2038. 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, 121 S.Ct. 2038.

**\*385** 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, 121 S.Ct. 2038. 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, 121 S.Ct. 2038 (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, 121 S.Ct. 2038. 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, 121 S.Ct. 2038 (quoting *Silverman v. U.S.*, 365 U.S. 505, 512, 81 S.Ct. 679, 5 L.Ed.2d 734 (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 \*386 of 28 days. — \*\*345 — U.S. —, 132 S.Ct. 945, 948, 181 L.Ed.2d 911 (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, 103 S.Ct. 1081, 75 L.Ed.2d 55 (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 \*387 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).

**\*\*346** 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* **\*388** –*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).

**\*389** [6] [7] 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, 121 S.Ct. 2038. 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 **\*\*347** 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 \*390 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 [*U.S. v. Chadwick, supra* [433 U.S. 1, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977) ]], rather than a container the size of the cigarette package in [*U.S. v. Robinson* [414 U.S. 218, 94 S.Ct. 467, 38 L.Ed.2d 427 (1973) ]].

*Id.* at 2489.

The State argues that its use of the Hailstorm here should be analogized to *Knotts*, 460 U.S. 276, 103 S.Ct. 1081, 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, 103 S.Ct. 1081. 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, 103 S.Ct. 1081. 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, 104 S.Ct. 3296. Rather, the information obtained in *Knotts* was “voluntarily conveyed to anyone who wanted to look[.]” *id.* (quoting *Knotts*, 460 U.S. at 281, 103 S.Ct. 1081), and the subsequent search warrant was also supported

by “intermittent visual surveillance” of the \*391 cabin, *Knotts*, 460 U.S. at 279, 103 S.Ct. 1081. 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, 121 S.Ct. 2038 (quoting \*348 *Boyd v. United States*, 116 U.S. 616, 628, 6 S.Ct. 524, 29 L.Ed. 746 (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, 103 S.Ct. 1081. 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.

\*392 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 Fed.Appx. 75 (4th Cir.2015).<sup>16</sup> 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 \*\*349 data, ... unquestionably implicate Fourth Amendment privacy rights.”); *In re 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 \*393 on their apparatus.”<sup>17</sup> Recognizing that the Fourth Amendment protects people and not simply areas, *Katz*, 389 U.S. at 353, 88 S.Ct. 507, we conclude that people have a reasonable expectation of privacy in real-time cell phone location information.

<sup>16</sup> 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>].

<sup>17</sup> 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, 88 S.Ct. 507.

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, 121 S.Ct. 2038. 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, 121 S.Ct. 2038 (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 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 \*394 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, 121 S.Ct. 2038 (declining to adopt a Fourth Amendment standard that \*\*350 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, 104 S.Ct. 3296 (“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 \*395 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**

[8] [9] 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, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) and *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (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, 99 S.Ct. 2577. 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, 99 S.Ct. 2577 (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 167, 98 S.Ct. 364, 54 L.Ed.2d 376 (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 \*396 “legitimate expectation of privacy” regarding the numbers he dialed on his phone.

*Id.* at 742, 99 S.Ct. 2577. 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 \*\*351 the ordinary course of business.” 425 U.S. at 442, 96 S.Ct. 1619.

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 carrying and using a cell phone that regularly communicates with nearby cell towers, Andrews assumed the risk that the information transmitted to the cell towers would be revealed to the police.

According to Andrews, the third-party doctrine of *Smith v. Maryland*, is inapplicable because “a cell phone user takes no conscious, voluntary action to constantly share location information with a third party.” Andrews maintains that the Supreme Court in *Smith* reached its conclusion using a specific line of reasoning, recognizing that “telephone subscribers ‘realize’ that they send dialed numbers to the telephone company” and by virtue of those numbers appearing on their monthly bills “subscribers ‘realize’ that the dialed numbers are recorded by the telephone company.” Andrews contends that the same cannot be said in the instant case. As Andrews points out, the Court in *Smith* focused on the actual knowledge attributed to telephone users and stated:

All 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. All subscribers realize, moreover, that the \*397 phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.

*Id.* at 742, 99 S.Ct. 2577. In that context, the court determined that because the “petitioner voluntarily conveyed to [the telephone company] information that it had facilities for recording and that it was free to record [,] ... petitioner assumed the risk that the information would be divulged to police.” *Id.* at 745, 99 S.Ct. 2577.

Although the Supreme Court's decision in *Smith* has been applied broadly, *see, e.g., United States v. Bynum*, 604 F.3d 161, 162–64 (4th Cir.2010) (upholding the government's use of a subpoena to obtain a website user's

name, email address, telephone number, and physical address—all information that the user entered on the website when he opened his account—from a website operator), it remains that a party must **voluntarily convey** information to a third-party, before there is no longer a reasonable expectation of privacy in that information. *Cf. Jones*, 132 S.Ct. at 957 (Sotomayor, J., concurring) (“This approach [in *Smith* ] 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.... I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.” (citation omitted)). Recently, in *United States v. Graham*, *supra*, the Fourth Circuit addressed the application of the third-party doctrine to CSLI and stated:

[The precedents] simply hold that a person can claim no legitimate expectation of privacy in information she voluntarily conveys to a third party. It is that voluntary conveyance—not the \*\*352 mere fact that the information winds up in the third party's records—that demonstrates an assumption of risk of disclosure and therefore the lack of any reasonable expectation of privacy. We decline to apply the third-party doctrine in the present case because a cell phone user does not “convey” CSLI to her service provider at all—voluntarily \*398 or otherwise—and therefore does not assume any risk of disclosure to law enforcement.

796 F.3d at 354 (footnote omitted).

We agree, once again, with the *Graham* court and join in the view shared by other courts that, “[t]he fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by ‘choosing’ to carry a cell phone must be rejected.” *Graham*, 796 F.3d at 355–56 (quoting *In re United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F.Supp.2d 113, 127 (E.D.N.Y.2011)). Cell phone users

do not actively submit their location information to their service provider.

In the present case, there was no affirmative act like “dialing.” This is made abundantly clear by Det. Haley’s testimony stating that “if they’re on the phone, then they’re already connected to ... the [ ] network[, a]nd we’re not going to be able to pull them off of that until ... they hang up the call.” Det. Haley’s testimony reveals that, in the event that an individual is actively using the cell phone to knowingly transmit signals to nearby cell towers, the cell site simulator will not be able to access the phone.

The pin-point location information that led to finding Andrews was obtained directly by law enforcement officers and not through a third-party. It is not the case that Andrews’s cell phone transmitted information to the service provider that was then recorded and shared with law enforcement. Thus, it cannot be said that Andrews “assumed the risk” that the information obtained through the use of the Hailstorm device would be shared by the service provider as in *Smith*. The function of the Hailstorm device foreclosed that possibility. When asked “how do you get information about where the phone is on the [Hailstorm] machine,” Det. Haley responded: “[W]hen [Hailstorm] captures that identifier that you put into the machine or the equipment, it then tells you ... where the signal’s coming from[.]” Under the facts of this case, the ultimate location data relied on by the police was never \*399 transmitted to a third party voluntarily by Andrews. Because there was no third-party element to the use of the Hailstorm by the BPD to locate Andrews, *Smith* is inapposite. We conclude the Third Party Doctrine does not apply in this case.

## II.

### Standing

[10] One of the State’s primary arguments on appeal is that Andrews lacks standing to challenge the search of 5032 Clifton Avenue. The State argues that once it challenged Andrews’s standing to protest the search of 5032 Clifton Avenue, the burden was on Andrews to put on evidence during the suppression hearing to establish Andrews’s “basis for claiming he had a reasonable expectation of privacy in the contents of someone else’s

home.” The State posits the suppression court erred in “finding that there was no need to prove standing.”

[11] Certainly, “[t]he burden is on the defendant to show standing; it is not on the State to show non-standing.” \*\*353 *State v. Savage*, 170 Md.App. 149, 177, 906 A.2d 1054 (2006). In *Savage*, however, this Court clarified that standing “[i]s exclusively a threshold question of applicability, concerned only with the coverage by the Fourth Amendment of the defendant who seeks to raise a Fourth Amendment challenge.” *Id.* at 174, 906 A.2d 1054. Thus, the burden on a proponent of a motion to suppress is to establish “that his own Fourth Amendment rights were violated by the challenged search or seizure.” *Id.* at 175, 906 A.2d 1054 (emphasis in *Savage*) (quoting *Rakas v. Illinois*, 439 U.S. 128, 130 n. 1, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978)).

Andrews points out that the State “failed to respond in any meaningful way” to his motion to suppress, and did not raise the issue of standing to challenge the search of 5032 Clifton Avenue until well into the June 4, 2015 suppression hearing. Andrews asserts that it was the State’s suggestion that the parties stipulate that the issues before the court be decided based on the transcripts, the arrest warrant, the pen register/trap \*400 & trace application, and the search warrant. Andrews contends the State did not raise the standing issue until after the fact-finding portion of the hearing had concluded. At that time, the court requested that Andrews address the issue, and defense counsel made a proffer that Andrews was an overnight guest at 5032 Clifton Avenue and offered to put him on the stand to provide supporting testimony.<sup>18</sup> Andrews argues that the State waived any argument regarding standing, pointing to the State’s delay, its failure to challenge his proffer, and its concession that its trial theory was the fact “that [Andrews] has some interest [in 5032 Clifton Avenue] and that is why the gun from this crime, the murder weapon, was there with him.”

<sup>18</sup> It is plain that an overnight guest has a legitimate expectation of privacy in his host’s home and “may claim the protection of the Fourth Amendment.” *Carter, supra*, 525 U.S. at 90, 119 S.Ct. 469; *Savage*, 170 Md.App. at 188–89, 906 A.2d 1054. As Andrews points out, defense counsel made a proffer that Andrews was an overnight guest and offered to put testimony to that effect on the record. The State has not seriously challenged Andrews’s connection

to the residence, but seeks merely to assert that his unopposed proffer was not sufficient to rebut their late challenge. We observe that—after the State sought to rely on earlier transcripts to provide necessary testimony, failed to challenge standing during the evidentiary portion of the suppression hearing, and left uncontroverted Andrews's proffer that he was an overnight guest—Andrews's proffer under the circumstances may have been sufficient to counter the State's standing argument.

We need not pursue the nuances of the parties' "standing" argument as they have framed the issue. We have already determined that Andrews had a reasonable expectation of privacy in his aggregate and real-time location information (CSLI) contained in his cell phone. See *Rakas*, 439 U.S. at 139–140, 99 S.Ct. 421 (stating that "the better analysis forthrightly focuses on the extent of a particular defendant's rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing[.]" and "[t]hat inquiry in turn requires a determination of whether the disputed search and seizure has infringed an interest of the defendant which the Fourth Amendment was designed to protect."). The search warrant search for 5032 Clifton Avenue \*401 was based solely on constitutionally tainted information. As the suppression court explained, "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 [is to] be suppressed, that's all that it is." Because the Fourth Amendment violation of Andrews's privacy in his real-time CSLI provided the only nexus to \*\*354 5032 Clifton Avenue, Andrews was entitled to challenge that search. See *Wong Sun v. United States*, 371 U.S. 471, 487–88, 83 S.Ct. 407, 9 L.Ed.2d 441 (1963) (stating that, in determining whether evidence is fruit of the poisonous tree, "the more apt question in such a case is whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint." (citation and internal quotation marks omitted)). For the foregoing reasons, Andrews had standing to challenge the "search" of 5032 Clifton Avenue.

### III.

## The Warrant Requirement

[12] Having determined that the government's use of a cell site simulator to obtain location information directly from an individual's cell phone is a "search" under the Fourth Amendment, and, therefore, requires a warrant based on probable cause, we now examine the state's reliance on the pen register/trap & trace order issued by the circuit court. First, we examine whether the Maryland pen register statute authorized the use of a cell site simulator. Second, we examine whether the putative pen register/trap & trace order in this case operated as the equivalent of a warrant as the State contends.

### a. The Maryland Pen Register Statute Does Not Authorize the Use of Cell Site Simulators Such as Hailstorm

The function of the Hailstorm device, as illuminated by testimony before the suppression court, places it outside the \*402 statutory framework of the Maryland pen register statute. The statute authorizes the use of the following surveillance methods defined in CJP § 10–4B–0.1:

#### Pen register

(c)(1) "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.

(2) "Pen register" does not include any device or process used:

(i) By a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by the provider or any device used by a provider or customer of a wire communication service for cost accounting or other similar purposes in the ordinary course of its business; or

(ii) To obtain the content of a communication.

#### Trap and trace device

(d)(1) "Trap and trace device" means a device or process that captures the incoming electronic or other

impulses that identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.

(2) “Trap and trace device” does not include a device or process used to obtain the content of a communication.

**Wire communication, electronic communication, and electronic communication service**

(e) “Wire communication”, “electronic communication”, and “electronic communication service” have the meanings stated in § 10–401 of this title.

The statute specifies that any order issued must identify, if known, “the person to whom is leased or in whose name is listed the **telephone line or other facility to which the pen register or trap and \*\*355 trace device is to be attached or applied.**” CJP § 10–4B–04(b)(1) (emphasis added).

**\*403** Construing the plain language of CJP § 10–4B–01, we determine that it does not, on its face, apply to the use of cell site simulators. A “pen register” is “a device or process that records ... signaling information transmitted by an instrument ... **from which a wire or electronic communication is transmitted.**” CJP § 10–4B–01(c)(1) (emphasis added). As discussed above, the Hailstorm device does not passively intercept an electronic communication that has been transmitted. Rather, it initiates contact with a cell phone and traces the signal received in response. A “trap and trace device” is a “device or process that captures the **incoming electronic or other impulses** that identify the originating number or other dialing, routing, addressing, and **signaling information reasonably likely to identify the source of a wire or electronic communication.**” CJP § 10–4B–01(d) (1) (emphasis added). The function of the Hailstorm device—to shower an electronic barrage of signals into a target area to actively engage the target cell phone—goes well beyond the bounds of the pen register statute which by its terms is limited to authorizing devices that record or identify the source of a communication or capture an originating number.

The Maryland pen register statute has been examined in only one reported opinion by a Maryland appellate court.<sup>19</sup> See *Chan v. State*, 78 Md.App. 287, 293, 552 A.2d 1351 (1989) (upholding the use of a trap and trace

device pursuant to a court order to obtain data from over 5,000 calls over an eighty- **\*404** day period). In *Chan*, although this Court determined that the newly enacted Maryland pen register statute was not applicable because it did not take effect until July 1, 1988, it stated that the new statute “unquestionably cover[ed]” the “trap and trace” of incoming calls and observed:

19 In the federal district court in *United States v. Wilford*, a defendant more recently argued that cell phone ping- ing was not authorized by Maryland’s pen register statute. 961 F.Supp.2d 740, 768 (D.Md.2013), *on reconsideration in part* (Nov. 27, 2013). In that case, the defendant maintained that the statutory language “is limited to providing law enforcement numbers that dialed into the target phone and numbers dialed out,” but does “not contemplate” the use of a cell phone as a “physical locator/tracking device.” *Id.* at 769. The district court noted that “[n]o judicial decision offers any guidance as to the scope of the Maryland statute with respect to ping- ing.” *Id.* However, rather than address whether the collection of CSLI was authorized by the pen register statute, the district court accepted that contention arguendo and, instead, based its holding on the unavailability of suppression as a remedy for violation of the statute. *Id.* at 770.

In response to the Electronic Communications Privacy Act of 1986 passed by the Federal Congress, the Maryland General Assembly moved for the first time to regulate “pen registers” and “trap and trace” devices by Chapter 607 of the Acts of 1988. The new regulation is not part of the “Wiretapping and Electronic Surveillance” subtitle but is a separate subtitle of its own, 4B, dealing with the distinct subject matter of “Pen Registers and Trap and Trace Devices.” **Its provisions and its wording are virtually verbatim with those of its Federal counterpart.**

*Id.* at 308, 552 A.2d 1351 (emphasis added).

In 2001, Congress amended the definition of the term “pen register” in the federal counterpart as part of the USA PATRIOT Act. See PL 107–56, October 26, 2001, 115 Stat. 272. Subsequently, in 2002, the Maryland pen register statute was also amended to the current versions, reproduced above. 2002 Md. Laws, ch. 100 **\*\*356** (H.B. 1036). Notably, since *Chan* was decided in 1989, the wording of the Maryland statute remains virtually verbatim with its federal counterpart. See 18 U.S.C. § 3127; 18 U.S.C. § 2510.

Looking then, at the federal statutory scheme, we note that the federal Communications Assistance for Law Enforcement Act (“CALEA”), which delineates a telecommunications carrier’s duty to cooperate in the interception of communications for law enforcement purposes, provides that “with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in [section 3127 of Title 18](#)), **such call-identifying information shall not include any information that may disclose the physical location of the subscriber** (except to the extent that the location may be determined from the telephone number).” [47 U.S.C. § 1002 \(2015\)](#) (emphasis added). Thus, federal law [\\*405](#) specifies that the federal equivalent to the Maryland pen register statute does not authorize location information. Rather, the federal scheme allows the government to use a mobile tracking device through warrant or other order as contemplated in [18 U.S.C. § 3117](#) and [Federal Rule of Criminal Procedure 41](#).

Although there are no reported opinions that address whether the collection of real-time cell site location information (CSLI) is authorized under the Maryland’s pen register statute, numerous federal courts construing the virtually identical federal statutes have found no statutory authorization for obtaining such information without demonstrating probable cause. In 2005, the United States District Court for the Southern District of Texas held that the government must demonstrate probable cause and obtain a search warrant to obtain real-time CSLI. *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, [396 F.Supp.2d 747, 759 \(S.D.Tex.2005\)](#). Construing the federal statutes, the district court stated:

Tracking device information such as cell site data is plainly not a form of electronic communication at all.

\* \* \*

This type of surveillance is unquestionably available upon a traditional probable cause showing under [Rule 41](#) [for a mobile tracking device]. On the other hand, permitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns, especially when the phone is monitored in the home or other places where privacy is reasonably expected.

*Id.* at 759, 765. See also *In re Application of the United States for an Order Authorizing Installation & Use of a Pen Register*, [415 F.Supp.2d 211, 219 \(W.D.N.Y.2006\)](#) (holding that the government was not entitled to real-time CSLI by statute and thus, was required to make a “showing that there exists probable cause to believe that the data sought will yield evidence of a crime.”). Directly addressing the use of a cell [\\*406](#) site simulator (such as Stingray or Hailstorm) to obtain real-time CSLI for tracking purposes, the District Court for the Southern District of Texas determined that, rather than merely capturing signaling information as contemplated in the federal pen register statute, the use of a cell site simulator constituted a mobile tracking device. *In re the Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, [890 F.Supp.2d 747, 752 \(S.D.Tex.2012\)](#).

We acknowledge that law enforcement has long relied on pen register/trap & trace orders for valid and vital investigative purposes. They will continue to do so. The pen register statute, however, is limited by its terms and is not intended to [\\*\\*357](#) apply to other, newer technologies. Thus we hold that a pen register/trap & trace order is not sufficient to authorize use of the Hailstorm.<sup>20</sup>

<sup>20</sup> Federal law enforcement agencies have recognized that they need to obtain warrants rather than rely on less rigorous legal authorizations before utilizing cell site simulators. On September 3, 2015, the United States Justice Department of Justice announced a new policy setting forth required practices with respect to the treatment of information collected through the use of cell site simulators and stated:

While the department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, **law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator.**

*Justice News, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, DOJ 15–1084 (2015) (emphasis added).

### **Criminal Procedure § 1–203.1**

Although at the time Andrews was arrested Maryland did not have a corollary to the provision in [Federal Rule of Criminal Procedure 41](#) that specifically authorizes issuance of a warrant for a mobile tracking device,

Maryland has since enacted a statute authorizing law enforcement to obtain real-time CSLI, effective October 1, 2014. Maryland Code (2001, 2008 Repl.Vol., 2014 Supp.) [Criminal Procedure Article \(“CP”\) § 1–203.1](#). The statute provides that a court may issue an order allowing an officer to obtain real-time location information from an electronic device based on probable cause that:

**\*407** (i) a misdemeanor or felony has been, is being, or will be committed by the owner or user of the electronic device or by the individual about whom location information is being sought; and

(ii) the location information being sought:

1. is evidence of, or will lead to evidence of, the misdemeanor or felony being investigated; or
2. will lead to the apprehension of an individual for whom an arrest warrant has been previously issued.

[CP § 1–203.1\(b\)\(1\)](#). The Fiscal and Policy Note prepared by the Department of Legislative Services for the General Assembly concerning this statute when it was first proposed, recognized that law enforcement officers were using the Maryland pen register statute to obtain cell phone-related information. It explained that the proposed statute would specifically authorize the capture of CSLI in accord with several recent federal court decisions finding that probable cause was needed to obtain such information. Fiscal and Policy Note (Revised), Senate Bill 698, Criminal Procedure—Electronic Device Location Information—Order (2014). The fiscal and policy note also contemplated the use of cell site simulators and stated:

While cell phone records are usually obtained from a cell phone provider, technology is making it possible for law enforcement to bypass these companies altogether. Certain devices allow law enforcement to obtain location data by imitating a cell phone tower, getting a phone to connect with it, and measuring signals from the phone to pinpoint its location. The device, which is being used by the Federal Bureau of Investigation, the military, and local law enforcement, is known by several trade names,

including StingRay, KingFish, and LoggerHead.

Notably, [CP § 1–203.1](#) contains safeguards and limitations not found in the Maryland pen register statute, including a thirty-day durational limit on the collection of location information unless an extension is sought on continuing probable cause, **\*\*358** and a provision requiring notice to the user or owner of the monitored device within 10 days absent a showing of good cause to delay. [CP § 1–203.1\(c\)](#) and (d).

**\*408** The parties have briefed extensively their view of the meaning and application of [CP 1–203.1](#). Other than to provide context for the history of the Maryland pen register statute and our conclusion that it was not intended to cover cell site simulators, we do not address the application of [CP 1–203.1](#) and decline to opine as to whether an order under [CP 1–203.1](#) will suffice to satisfy the requirements of a warrant based on probable cause.

In sum, we conclude that the purpose of Maryland's pen register statute is to capture information resulting from two-way, electronic or wire communications. Nothing in the plain language of [CJP § 10–4B–01 et seq.](#) suggests that it was ever intended to allow surveillance technology that can exploit the manner in which a cell phone transmits data to convert it into a mobile tracking device. Accordingly, an order issued pursuant to [CJP § 10–4B–04](#) cannot authorize the use of a cell site simulator, such as Hailstorm. Because there was no statutory authorization for the BPD's use of the Hailstorm cell site simulator, we hold that the BPD should have sought a warrant or a specialized order upon a particularized showing of probable cause, and based on sufficient information about the technology involved to permit the court to contour reasonable limitations on the scope and manner of the BPD's use of the device.<sup>21</sup> See, e.g., *In re Application of the United States for an Order Authorizing Installation & Use of a Pen Register*, 415 F.Supp.2d at 219.

<sup>21</sup> To the extent that the State makes a limited argument that there is no suppression remedy available for violation of the [sections 10–4B–01 et seq.](#), we respond simply that the circuit court found, and we agree, that the use of the cell site simulator was a Fourth Amendment violation and, thereby, the exclusionary rule applies. The fact that there may have been a

contemporaneous violation of [sections 10-4B-01 et seq.](#) does not limit the available remedy.

**b. The Order Obtained by the State Was Not Equivalent to a Warrant**

[13] The State insists that its use of the Hailstorm device to track Andrews's cell phone was authorized by the court \*409 order. In the absence of a specific statute that would have authorized the use of a cell site simulator at the time Andrews was arrested, the State presses that “the police erred on the side of caution and obtained a court order specifically authorizing the use of a cellular tracking device to find Andrews's phone [.]” pursuant to the “nearest analog”—the Maryland pen register statute. The State acknowledges that the court order described in the Maryland pen register statute does not use the words “warrant” or “probable cause.” Nevertheless, the State argues that, in this case, the BPD's application and the resulting order “went far beyond the requirements of the statute.”

The State points out that the BPD application was for an order allowing the police

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 [...] and shall initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonabl[y] available ...

The State also notes that the resultant order states that probable cause exists to authorize the use of a “Cellular Tracking Device.” Thus, the State contends that \*\*359 because the pen register\trap & trace order stated that it was based upon a finding of probable cause, it was, therefore, “the functional equivalent of a warrant.”

Andrews emphasizes that the order may issue on just a showing “that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation.” CJP § 10-4B-04(a)(1). In addition to the fact that a pen register\trap & trace order does not contemplate the use of a cell site simulator, Andrews

points out that it also does not satisfy the requirements that a warrant based on probable cause be attached to a specific suspected crime, be confined in scope, or describe with particularity the place to be searched or the person to be seized. Andrews contends that “[t]he \*410 moment BPD conducted surveillance with something other than a pen register, it exceeded the purview of the pen register order.” Further, Andrews contends that BPD's application “For an Order Authorizing the Installation and Use of a Device Known as a Pen Register/Trap & Trace,” was intentionally captioned to ensure that the circuit court scrutinized it according to the statutory pen register factors. Andrews argues that BPD's “disingenuous efforts” hid from the circuit court “the scope, intensity, [and] nature of the search,” and prevented the court from conducting a proper probable cause analysis.

We begin with our appraisal that an order issued under the pen register statute is not the equivalent of a warrant based on probable cause—a fact the State implicitly concedes in its argument that it “went beyond the requirement of the statute.” The applicable requirements of the statute are contained first in § 10-4B-03:

(b) *Contents.*—An application under subsection (a) of this section shall include:

- (1) The identity of the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
- (2) A statement under oath by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Additionally, 10-4B-04(a) states that an order may issue if the court finds the information likely to be obtained by the device is relevant to an ongoing criminal investigation, and the order must:

- (3) Specify the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of a trap and trace device, the geographic limits of the trap and trace order;

**\*411** (4) Contain a description of the offense to which the information likely to be obtained by the pen register or trap and trace device relates[.]

CJP § 10-4B-04(b)(3) and (4). Plainly, this limited showing falls short of the particularity required for the issuance of a search warrant. See *Illinois v. Gates*, 462 U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983) (“The task of the issuing magistrate is simply to make a practical, common-sense decision whether ... there is a fair probability that contraband or evidence of a crime will be found in a particular place.”); *Nero v. State*, 144 Md.App. 333, 345-46, 798 A.2d 5 (2002) (“General warrants, of course, are prohibited by the Fourth Amendment.... [T]he problem [posed by the general warrant] is not that of intrusion per se, but of a general, exploratory rummaging in a person's **\*\*360** belongings.... [The Fourth Amendment addresses the problem] by requiring a ‘particular description’ of the things to be seized.” (quoting *Andresen v. Maryland*, 427 U.S. 463, 480, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976))).

Moving to the State's argument that the order was sufficient because it went beyond the requirements of the statute, we start by rejecting the State's contention that the words “probable cause” contained in the pen register application and order converted the overreaching order into a warrant. The “probable cause” articulated in the resulting order is merely that **“information likely to be obtained ... is relevant to an ongoing criminal investigation.”** (Emphasis in original). Certainly, while this reflects the standard required for issuance of an order under CJP § 10-4B-04, it falls far short of the particularity required to support a search warrant. See *Gates*, 462 U.S. at 238, 103 S.Ct. 2317; *Nero*, 144 Md.App. at 345-46, 798 A.2d 5.

In the information “offered in support of probable cause” the application states:

Your Applicant hereby certifies that the information likely to be obtained concerning [Andrews's] location will be obtained by learning the numbers, locations and subscribers of the telephone number(s) being dialed or pulsed from or to **\*412** the aforesaid telephone and that

such information is relevant to the ongoing criminal investigation.

Plainly, the State's use of the Hailstorm device extended far beyond this certification as to how information concerning Andrews's location would be obtained.

Here, the State inserted language into its application and proposed order attempting to, without being specific, obtain court authorization for more than a pen register \trap & trace order. Although the application does request authorization to use a “Cellular Tracking Device,” it fails to name or describe any cell site simulator. In fact, there is absolutely nothing in the application or order that identifies the Hailstorm device, or provides even a rudimentary description of cell site simulator technology. The application also failed to identify any geographical limitation to the BPD's use of the undisclosed surveillance technology, and did not explain what was to be done with the information collected. Nor did the application disclose the possibility that the technology employed may capture the cell phone information (unique serial numbers) of innocent third parties in range of the target area. Finally, we are troubled that the application for a pen register \trap & trace order did not fully apprise the circuit court judge from whom it was sought of the information that it would yield. Based on the application that he received, the circuit judge was entitled to expect that the results would be a list of telephone numbers that Andrews called and that called Andrews—not a real-time fix on his location.

We determine that the pen register \trap & trace order in this case failed to meet the requirements of a warrant. To allow the government to collect real-time location information on an unknown number of private cell phones, without any geographic boundaries, without any reporting requirements or requirements that any unrelated data be deleted, and without a showing of probable cause that contraband or evidence of a particular crime will be found through the particular manner in which the search is conducted would certainly run afoul of the Fourth Amendment. As stated in our holding above, **\*413** unless a valid exception to the warrant requirement **\*\*361** applies,<sup>22</sup> the government may not use a cell phone simulator without a warrant or, alternatively, a specialized order that requires a particularized showing of probable cause, based on sufficient information about the technology involved to allow a court to contour reasonable limitations on the scope and manner of

the search, and that provides adequate protections in case any third-party cell phone information might be unintentionally intercepted. To hold otherwise would be to abandon the Fourth Amendment by assuming, without any foundation, that the citizens of Maryland have forfeited their reasonable expectation of privacy in their personal location.

22 One of the exceptions more commonly relied upon applies when “ ‘the exigencies of the situation’ make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.” *Kentucky v. King*, 563 U.S. 452, 460, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011) (some internal quotation marks omitted) (quoting *Mincey v. Arizona*, 437 U.S. 385, 394, 98 S.Ct. 2408, 57 L.Ed.2d 290 (1978)). Maryland has recognized that “[e]xigent circumstances exist when a substantial risk of harm to the law enforcement officials involved, to the law enforcement process itself, or to others would arise if the police were to delay until a warrant could be issued.” *Williams v. State*, 372 Md. 386, 402, 813 A.2d 231 (2002) (citations omitted). It remains the State’s burden to establish exigent circumstances sufficient to justify a warrantless search. *Wengert v. State*, 364 Md. 76, 85, 771 A.2d 389 (2001) (citations omitted). We note that the Supreme Court in *Riley*, *supra*, rejected the argument that officer safety, in that case, presented an exigent circumstance that justified officer’s accessing content on a cell phone seized in a search incident to arrest. The Court observed that “[t]o the extent dangers to arresting officers may be implicated in a particular way in a particular case, they are better addressed through consideration of case-specific exceptions to the warrant requirement, such as the one for exigent circumstances.” 134 S.Ct. at 2486.

#### IV.

##### The Exclusionary Rule

###### a. The Search Warrant Does Not Survive Removal of the Constitutionally Tainted Information.

[14] The State contends that the search warrant that was obtained for 5032 Clifton Avenue was valid because probable cause existed once “Andrews was found in the home.” According \*414 to the State, Andrews was arrested pursuant to a valid arrest warrant and the police had “the consent of the apparent owner of the home to

enter the home to take Andrews into custody.” Thus, the State argues, “[n]othing about the way in which Andrews was located negated the probable cause to believe that there could be evidence of the crimes at that address.”

In riposte, Andrews avers that without the location data provided by the cell site simulator, “the BPD possessed no nexus between the criminal activity at hand and 5032 Clifton Avenue.” Andrews asserts that, “[b]ecause the search warrant relied entirely on that nexus, it withers as fruit of the poisonous tree.”

First, we note that where entry into a protected space “was demanded under color of office” and “granted in submission to authority,” that submission does not equate to a waiver of a constitutional right. *Johnson, supra*, 333 U.S. at 13, 68 S.Ct. 367 (citing *Amos v. United States*, 255 U.S. 313, 41 S.Ct. 266, 65 L.Ed. 654 (1921)). Thus, the existence of an arrest warrant and the consent of the owner of the residence do not, in themselves, diminish Andrews’s protection under the Fourth Amendment. Nor do they render the later-acquired search warrant unassailable.

Second, the courts of Maryland have recognized that where a search warrant relies on information obtained in violation \*\*362 of the constitution, the question is “whether ‘after the constitutionally tainted information is excised from the warrant, the remaining information is sufficient to support a finding of probable cause.’ ” *Redmond v. State*, 213 Md.App. 163, 191–92, 73 A.3d 385 (2013) (quoting *Williams v. State*, 372 Md. 386, 419, 813 A.2d 231 (2002)). See also *Karo*, 468 U.S. at 720–21, 104 S.Ct. 3296 (stating that in determining whether evidence seized pursuant to a contested warrant remains admissible, one of the pertinent questions is whether “the warrant affidavit, after striking the [constitutionally tainted] facts ... contained sufficient untainted information to furnish probable cause for the issuance of the search warrant.”) Here, there \*415 can be no doubt that the only information linking Andrews and 5023 Clifton Avenue was the fruit of the Fourth Amendment violation. The State presents no credible argument that evidence of Andrew’s presence in the home was obtained by independent lawful means.

In *Redmond v. State*, the BPD were investigating an armed robbery in which a cell phone was stolen. 213 Md.App. at 169, 73 A.3d 385. During their investigation, detectives contacted the victim’s mobile service provider and, “by

triangulating the signal from cell phone towers in the area, determined that the stolen cell phone was in the proximity of 3303 Round Road.” *Id.* at 169, 73 A.3d 385. Thereafter, detectives began moving from house to house in the area, speaking to residents using a ruse that they were “looking for a pedophile named ‘Leroy Smalls.’ ” *Id.* at 170, 73 A.3d 385. After obtaining consent to enter the appellant’s residence under those false pretenses, one of the detectives surreptitiously dialed the number of the stolen cell phone, heard it ringing upstairs, and then walked through the entire house conducting a “protective sweep” including opening closet doors and checking under beds. *Id.* at 171, 73 A.3d 385. Officers then sought a search warrant for the home on the basis of what they had discovered in the home. *Id.* at 171–72, 73 A.3d 385.

After a careful analysis, we determined that “[b]y dialing the number of the stolen cell phone and walking upstairs to locate it, the police exceeded the scope of any consent that was given to their presence inside 3303 Round Road.” *Id.* at 189–90, 73 A.3d 385. Applying the exclusionary rule, we noted that “all the information ... attested to in applying for the search warrant (and on which the search warrant was granted) ... was discovered during the initial illegal entry.” *Id.* at 192, 73 A.3d 385. We determined that the search warrant was not issued based on an independent lawful source and the unlawfully obtained evidence should be suppressed.<sup>23</sup> \*\*363 *Id.* And, \*416 we soundly rejected the argument that evidence in a warrant application was obtained by independent lawful means “(1) where the officer’s decision to seek the warrant was prompted by what they had seen during the initial entry; and (2) where information obtained during that entry was presented to the [judge] and affected his [or her] decision to issue the warrant.” *Id.* at 191, 73 A.3d 385 (internal quotation marks omitted) (alterations in *Redmond*) (quoting *Kamara v. State*, 205 Md.App. 607, 627–28, 45 A.3d 948 (2012)). See also *Murray v. United States*, 487 U.S. 533, 534, 108 S.Ct. 2529, 101 L.Ed.2d 472 (1988) (“The ultimate question is whether the search pursuant to warrant was in fact a genuinely independent source of the information and tangible evidence at issue. This would not have been the case if the agents’ decision to seek the warrant was prompted by what they had seen during the initial entry or if information obtained during that entry was presented to the Magistrate and affected his decision to issue the warrant.”).

23

Although the warrant application in *Redmond* mentioned reliance on “sophisticated mobile and/or portable surveillance equipment” to locate the stolen cell phone, in that case we observed that:

Detective Jendrek did not testify that the ATT used *any* “sophisticated mobile and/or portable surveillance equipment” while in the 3300 block of Round Road. Rather, his testimony was that the ATT detectives confirmed the precise location of the cell phone by use of ordinary police investigatory tactics: speaking to the occupants of two houses, dialing the number of the stolen cell phone, listening for it to ring, and, ultimately, physically observing the stolen cell phone lying on a dresser.

Thus, to the extent that the averments in the search warrant application represent that the ATT detectives used “sophisticated” means to locate the stolen cell phone while at the scene on the afternoon of March 2, 2010, they are simply inaccurate.

213 Md.App. at 193, 73 A.3d 385. The defendant in *Redmond* did not challenge the use of any such device or the use of cell tower information. Accordingly, in *Redmond* we did not address the use of sophisticated mobile surveillance systems, as we must in the matter *sub judice*.

As in *Redmond*, here, the evidence that forms the only basis for probable cause in the State’s search warrant application—that Andrews was at 5032 Clifton Avenue—was that obtained through an unlawful search—in this case, the BPD’s use of the Hailstorm device. We agree with the circuit court’s determination that there was no independent lawful source to establish a nexus between Andrews and the residence. *Cf. Agurs v. State*, \*417 Md. 62, 84, 998 A.2d 868 (2010) (stating that “police should have been aware that there must be a nexus between criminal activity and the place to be searched.”). Accordingly, once the constitutional taint is removed from the search warrant in this case, what remains is insufficient to establish probable cause for a search of 5032 Clifton Avenue and, as discussed further *infra*, the evidence seized in that search withers as the fruit of the poisoned tree. *Franks v. Delaware*, 438 U.S. 154, 156, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978) (stating that if “the affidavit’s remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.”). Therefore, we affirm the suppression court’s exclusion of all evidence found at 5032 Clifton Avenue.

### b. The State Cannot Rely on the Good Faith Exception

[15] Finally, the State argues that BPD's relied in good faith on the search warrant issued for 5032 Clifton Avenue after locating Andrews inside that address. The State asserts that police officers relied on, first, the pen register \trap & trace order, and, second, on the later issued search warrant for the premises. The State maintains that “[t]his is good faith squared [.]” and there is “simply no officer misconduct to deter in this case.” Thus, the State contends that the exclusionary rule should not apply in this case.

Andrews contends that without the location information provided by the cell site simulator the BPD possessed no nexus between him and 5032 Clifton Avenue, and, “[b]ecause the search warrant relied entirely on that nexus, it withers as the fruit of the poisonous tree.” Andrews asserts that where the information relied on to obtain a warrant is the product of a Fourth amendment violation, the fruit of the poisonous tree doctrine trumps the good faith exception. Moreover, Andrews argues that good faith cannot apply where “law enforcement officers, from the outset, dealt dishonestly with the judiciary.”

\*418 In *United States v. Leon*, the Supreme Court held that, where officers have acted in good faith pursuant to a warrant that \*\*364 was later discovered to be invalid, exclusion is not warranted to deter police over-reach or misconduct. 468 U.S. 897, 924, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). The Supreme Court cautioned, however, that

[t]he good-faith exception for searches conducted pursuant to warrants is not intended to signal our unwillingness strictly to enforce the requirements of the Fourth Amendment, and we do not believe that it will have this effect. As we have already suggested, the good-faith exception, turning as it does on objective reasonableness, should not be difficult to apply in practice. When officers have acted pursuant to a warrant, the prosecution should ordinarily be able to establish objective good faith without a substantial expenditure of judicial time.

In *Fitzgerald v. State*, this Court aptly summarized the “good faith” exception:

Because the only purpose of the Exclusionary Rule of *Mapp v. Ohio*, 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961), is to deter unreasonable police behavior, *Leon* and [*Massachusetts v. Sheppard*, 468 U.S. 981, 104 S.Ct. 3424, 82 L.Ed.2d 737 (1984)] held that a mistake made by a judge in issuing a warrant should not be attributed to the police officer who executes it. Because the officer has been reasonable in relying on the judge's legal expertise, it would serve no deterrent purpose to exclude otherwise competent, material, and trustworthy evidence. See *Connelly v. State*, 322 Md. 719, 720–21, 589 A.2d 958 (1991).

153 Md.App. 601, 655–56, 837 A.2d 989 (2003) *aff'd*, 384 Md. 484, 864 A.2d 1006 (2004). However, this Court observed that in *Karo, supra*, the Supreme Court instructed that, if the information obtained through a Fourth Amendment violation “proved critical to establishing probable cause for the issuance of the warrant,” it would invalidate the subsequent search warrant for the house. *Id.* at 656, 837 A.2d 989 (citing *Karo, supra*, 468 U.S. at 719, 104 S.Ct. 3296). Accordingly, “the conclusion may readily be drawn that in the case of an \*419 antecedent Fourth Amendment violation which contributes to a warrant application, the ‘fruit of the poisoned tree’ doctrine ‘trumps’ the officer's ‘good faith’ reliance under *Leon* and *Sheppard*.” *Id.*

Here, as we noted above, the BPD submitted an overreaching pen register\trap & trace application that failed to clearly articulate the intended use, i.e., to track Andrews's cell phone using an active cell site simulator. The ensuing order did not support the use of the Hailstorm device, nor did it, in any way, serve as a de facto warrant for the use of the Hailstorm device. As the State's May 15, 2015 supplemental disclosure made clear, “WATF did not have the Clifton Ave address as a possible location until ATT provided that information.” Only after receiving that information through the use of the Hailstorm device and arresting Andrews at the premises did the same

BPD officers who submitted the pen register/trap & trace application then apply for a search warrant.

As Andrews points out, without the antecedent Fourth Amendment violation the nexus between the residence to be searched and the alleged criminal activity could not have been established. Cf. *Agurs*, 415 Md. at 84, 998 A.2d 868 (stating that “police should have been aware that there must be a nexus between criminal activity and the place to be searched.”). In the present case, the antecedent Fourth Amendment violation was the only basis upon which the search warrant application stood, and the fruit of the poisoned tree \*\*365 doctrine does, indeed, trump alleged good faith reliance on the part of BPD. See *Fitzgerald*, 153 Md.App. at 656, 837 A.2d 989.

The Supreme Court in *Leon*, was clear that “the officer’s reliance on the magistrate’s probable-cause determination and on the technical sufficiency of the warrant he issues must be objectively reasonable.” 468 U.S. at 922, 104 S.Ct. 3405. See, e.g., *Spence v. State*, 444 Md. 1, 12–13, 118 A.3d 864 (2015) (wherein the police officer, in searching a cell phone and reading text messages during a search incident to arrest, was \*420 acting in good faith reliance on then-controlling authority in Maryland); *Agurs*, 415 Md. at 83, 998 A.2d 868 (concluding that the good faith exception did not apply where “no reasonably well-trained police officer could have relied on the warrant that authorized the search of Agurs’ home.”). We cannot say the BPD officers in this case reasonably relied on the warrant obtained through their own misleading order application and unconstitutionally intrusive conduct. To do so would

allow law enforcement to insulate its own errors merely by presenting limited information to a magistrate, obtaining a warrant post-intrusion, and then re-entering the place to be searched. The good faith exception to the exclusionary rule seeks to avoid “[p]enalizing the officer for the magistrate’s error, rather than his own.” *Leon*, 468 U.S. at 921, 104 S.Ct. 3405. That is, however, not that case here. See *id.* at 919, 104 S.Ct. 3405 (“The deterrent purpose of the exclusionary rule necessarily assumes that the police have engaged in willful, or at the very least negligent, conduct which has deprived the defendant of some right. By refusing to admit evidence gained as a result of such conduct, the courts hope to instill in those particular investigating officers, or in their future counterparts, a greater degree of care toward the rights of an accused.” (quoting *United States v. Peltier*, 422 U.S. 531, 539, 95 S.Ct. 2313, 45 L.Ed.2d 374 (1975))).

It is for all of these reasons that we hold that the evidence obtained in the search of 5032 Clifton Avenue is inadmissible as fruit of the poisoned tree and was properly excluded by the suppression court.

**JUDGMENTS OF THE CIRCUIT COURT FOR BALTIMORE CITY AFFIRMED.**

**COSTS TO BE PAID BY MAYOR AND CITY COUNCIL OF BALTIMORE.**

**All Citations**

227 Md.App. 350, 134 A.3d 324