

**IN THE
COURT OF SPECIAL APPEALS OF MARYLAND**

SEPTEMBER TERM, 2015

NO. 1496

STATE OF MARYLAND,

Appellant

v.

KERRON ANDREWS,

Appellee

**APPEAL FROM THE CIRCUIT COURT FOR BALTIMORE CITY
(JUDGE KENDRA Y. AUSBY PRESIDING AT A SUPPRESSION HEARING)**

MOTION TO DISMISS AND APPELLEE'S BRIEF & APPENDIX

**PAUL B. DEWOLFE
Public Defender**

**DANIEL KOBRIN
Assistant Public Defender**

**Office of the Public Defender
Appellate Division
6 Saint Paul Street, Suite 1302
Baltimore, Maryland 21202-1608
P: (410) 767-2307
F: (410) 333-8801
DKobrin@opd.state.md.us**

Counsel for Appellee

INDEX

Table of Contents

| | Page |
|--|------|
| Motion to Dismiss..... | 1 |
| Statement of the Case | 5 |
| Questions Presented..... | 5 |
| Statement of Facts | 6 |
| Argument..... | 10 |
| i. THE SUPPRESSION COURT’S FINDINGS OF FACT WERE SUPPORTED DIRECTLY BY THE TESTIMONY OF THE STATE’S WITNESS..... | 12 |
| II. THE SUPPRESSION COURT CORRECTLY RULED THAT THE USE OF A CELL SITE SIMULATOR TO TRACK THE PRECISE LOCATION OF A CELL PHONE CONSTITUTED A “SEARCH” WITHIN THE MEANING OF THE FOURTH AMENDMENT. | 18 |
| a. Use of a Hailstorm to evaluate cellular activity inside of a home is a search. | 19 |
| b. Use of a Hailstorm to wirelessly capture location information from a cell phone is a search and seizure..... | 27 |
| c. The third-party doctrine cannot excuse the BPD’s searches in this case..... | 35 |
| d. A Maryland pen register trap/trace order is not warrant; the order in this case cannot authorize a Fourth Amendment search. | 43 |
| III. THE SUPPRESSION COURT CORRECTLY RULED THAT THE FRUIT OF THE HAILSTORM SEARCH WAS INADMISSIBLE AT MR. ANDREWS’ TRIAL..... | 47 |
| a. There is no issue with standing. | 48 |

b. The subsequent search warrant was fruit of the
poisonous tree.....51

c. Good faith is not applicable.53

Conclusion..... 54

Pertinent authority 55

Appendix

Memorandum Re: Purchase Wireless Collection Equipment/Technology and Non-
Disclosure Obligations executed by FBI, BPD, and City SAO.....Apx. 1

BPD Response to Maryland Public Information Act Request.....Apx. 6

Table of Citations

| | Page |
|--|--------|
| Cases | |
| <i>In re Application of the United States for an Order Authorizing Disclosure of Location Information for a Specified Wireless Telephone</i> , 849 F.Supp.2d 526 (D. Md. 2011) | 30 |
| <i>Agurs v. State</i> , 415 Md. 62 (2010)..... | 44 |
| <i>Berger v. New York</i> , 388 U.S. 41 (1967)..... | 34, 44 |
| <i>Boyd v. United States</i> , 116 U.S. 616 (1967)..... | 29 |
| <i>Brewer v. State</i> , 220 Md. App. 89 (2014) | 10, 16 |
| <i>Carroll v. United States</i> , 267 U.S. 132 (1925) | 24 |
| <i>City of Ontario, Cal v. Quon</i> , 560 U.S. 746 (2010) | 39 |
| <i>Collins v. State</i> , 138 Md. App. 300 (2001)..... | 51 |
| <i>Commonwealth v. Augustine</i> , 4 N.E.3d 846 (Mass. 2014)..... | 38 |
| <i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971)..... | 18 |
| <i>Fitzgerald v. State</i> , 153 Md. App. 601 (2003)..... | 54 |
| <i>Fitzgerald v. State</i> , 384 Md. 484 (2004) | 20, 21 |
| <i>Florida v. Jardines</i> , 133 S. Ct. 1409 (2013)..... | 20 |
| <i>Georgia v. Randolph</i> , 547 U.S. 103 (2006)..... | 20 |
| <i>Harris v. United States</i> , 331 U.S. 145 (1947) | 44 |
| <i>Holmes v. State</i> , 368 Md. 506 (2002)..... | 11 |
| <i>Illinois v. Gates</i> , 462 U.S. 213 (1983)..... | 44, 53 |
| <i>In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government</i> , 620 F.3d 304 (3d Cir. 2010) | 38 |
| <i>Joyner v. State</i> , 208 Md. App. 500 (2012) | 50 |

| | |
|--|------------|
| <i>Katz v. United States</i> , 389 U.S. 347 (1967)..... | 19, 44 |
| <i>King v. State</i> , 425 Md. 550 (2012) | 39 |
| <i>Kyllo v. United States</i> , 533 U.S. 27 (2001) | passim |
| <i>LeClair v. Hart</i> , 800 F.2d 692 (7th Cir. 1986) | 34 |
| <i>Minnesota v. Carter</i> , 525 U.S. 83 (1998)..... | 19, 48 |
| <i>Mobuary v. State</i> , 435 Md. 417 (2013) | 45 |
| <i>Nero v. State</i> , 144 Md. App. 333 (2002) | 44 |
| <i>Oliver v. United States</i> , 466 U.S. 170 (1984)..... | 20 |
| <i>Patterson v. State</i> , 401 Md. 76 (2007)..... | 44 |
| <i>Payton v. New York</i> , 445 U.S. 573 (1980)..... | 20 |
| <i>Peters v. State</i> , 224 Md. App. 306 (2015) | 44 |
| <i>Redmond v. State</i> , 213 Md. App. 163 (2013)..... | 11, 51, 52 |
| <i>Riley v. California</i> , 134 S.Ct. 2473 (2014)..... | passim |
| <i>Silverman v. United States</i> , 365 U.S. 505 (1961)..... | 20, 21, 36 |
| <i>Smith v. Maryland</i> , 442 U.S. 735 (1979)..... | passim |
| <i>Spence v. State</i> , 444 Md. 1 (2015)..... | 18 |
| <i>State v. Brooks</i> , 148 Md. App. 374 (2002)..... | 13 |
| <i>State v. Carter</i> , 630 N.E.2d 355 (Ohio 1994)..... | 54 |
| <i>State v. DeWitt</i> , 910 P.2d 9 (Ariz. 1996)..... | 54 |
| <i>State v. Earls</i> , 70 A.3d 630 (N.J. 2013)..... | 38 |
| <i>State v. Johnson</i> , 716 P.2d 1288 (Idaho 1986)..... | 54 |
| <i>State v. Klingenstein</i> , 92 Md. App. 325 (1992) | 52 |
| <i>State v. Payne</i> , 440 Md. 680 (2014) | 34, 41 |
| <i>State v. Scull</i> , 639 So.2d 1239 (La. Ct. App. 1994) | 54 |

| | |
|--|----------------|
| <i>States v. Grubbs</i> , 547 U.S. 90 (2006) | 44 |
| <i>Thompson v. State</i> , 139 Md. App. 501 (2001)..... | 51 |
| <i>Tracey v. State</i> , 152 So.3d 504 (Fla. 2014) | passim |
| U.S. Const., amend IV | 47 |
| <i>United State v. Leon</i> , 468 U.S. 897 (1984)..... | 53 |
| <i>United States v. Graham</i> , 796 F.3d 332 (4th Cir. 2015) | passim |
| <i>United States v. Jacobsen</i> , 466 U.S. 109 (1984) | 34 |
| <i>United States v. Jones</i> , 132 S. Ct. 945 (2012) | 29, 31, 32, 35 |
| <i>United States v. Karo</i> , 468 U.S. 705 (1984)..... | passim |
| <i>United States v. Knotts</i> , 460 U.S. 276 (1983)..... | 22 |
| <i>United States v. McGough</i> , 412 F.3d 1232, (11th Cir. 2005)..... | 54 |
| <i>United States v. Scales</i> , 903 F.2d 765 (10th Cir. 1990) | 54 |
| <i>United States v. Vasey</i> , 834 F.2d 782 (9th Cir. 1987) | 54 |
| <i>Williams v. State</i> , 372 Md. 386 (2002) | 51, 52 |
| <i>Williamson v. State</i> , 413 Md. 521 (2010)..... | 19 |

Constitutional Provisions

| | |
|------------------------------|--------|
| U.S. Const., amend. IV | 18, 20 |
|------------------------------|--------|

Statutes

| | |
|--|--------|
| Md. Code (2015 West), Courts & Judicial Proceedings Article, § 10-4B | 44, 45 |
| Md. Code (2015 West), Criminal Procedure Article, § 1-203 | 45 |

Rules

| | |
|------------------------|---|
| Md. Rule 4-252(f)..... | 9 |
|------------------------|---|

Md. Rule 8-604..... 51

Miscellaneous

Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 *Harvard J. Law & Tech.* 1 (2014) 17

Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 *Mich. L. Rev.* 561 (2009)..... 35

Pew Research Center (Pew Report), *Mobile Technology Fact Sheet*, <http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/> (last accessed December 29, 2015) 39

Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Nov. 12, 2014, http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_.... 40

Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap*, 16 *Yale J. Law & Tech* 134 (2013)..... 18, 33

U.S. Dep't of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, <http://www.justice.gov/opa/file/767321/download> (last accessed Dec. 30, 2015) 47

Wayne R. Lafave, 1 *Search and Seizure: A Treatise on the Fourth Amendment*, (5th ed. 2015)..... 35, 53

**IN THE
COURT OF SPECIAL APPEALS OF MARYLAND**

SEPTEMBER TERM, 2015

NO. 1496

STATE OF MARYLAND,

Appellant

v.

KERRON ANDREWS,

Appellee

**APPEAL FROM THE CIRCUIT COURT FOR BALTIMORE CITY
(JUDGE KENDRA Y. AUSBY PRESIDING AT THE SUPPRESSION HEARING)**

MOTION TO DISMISS

Appellee, by counsel, Daniel Kobrin, Assistant Public Defender, moves this Court pursuant to Maryland Rules 8-602(a)(3) & 8-603(c) to dismiss the instant appeal because the notice of appeal was not filed with the lower court within the time prescribed by Maryland Rule 8-202. In support, Appellee avers:

1. This appeal arises from a ruling of the Circuit Court of Baltimore City, J. Ausby presiding, suppressing the fruit of an illegal search pursuant to the Fourth Amendment to the United States Constitution. The suppression court issued its ruling from the bench after a hearing on August 20, 2015.


2. Pursuant to § 12-302(c)(4)(ii) of the Maryland Code (2015 West), Courts and Judicial Proceedings Article, the State was required to note its appeal no more than “15 days after the decision [was] rendered.” In this case, the 15-day deadline arrived on September 4, 2015.
3. On September 3, 2015, at 11:29 a.m., the State filed a notice of appeal in this case. Four hours later, at 3:44 p.m., the State filed an amended notice. As far as Appellee can tell, the amended notice changed only the citation to the statute granting the State authority to appeal a suppression ruling of constitutional dimension.
4. The certificate of service appended to both notices was defective. The certificate of service, signed by “Assistant State’s Attorney for Baltimore City,” fails to certify service on any entity. The certificate is merely left blank. No other admission or waiver of service was provided.
5. Pursuant to Maryland Rule 1-323, “[t]he clerk shall not accept for filing any pleading or other paper requiring service, other than an original pleading, unless it is accompanied by an admission or waiver of service or a signed certificate showing the date and manner of making service. A certificate of service is prima facie proof of service.”
6. The clerk of the circuit court was not permitted to accept for filing the State’s notice of appeal and amended notice because of the defective certificate. *Lovero v. DaSilva*, 200. Md. App. 433, 447 (2011). “A notice of appeal that fails to comply with the proof of service requirement under Rule 1–323 is not

‘filed’ within the meaning of Rule 8–202(a), notwithstanding the delivery to and acceptance by the clerk of such defective notice.” *Id.* at 449.

7. A copy of the amended notice was delivered by State’s Attorney Delivery to the Felony Trial Unit of the Maryland Office of the Public Defender in Baltimore City on September 4, 2015. The clerk of the Circuit Court did not know this, nor could have known this, when the notice and amended notice were filed one day earlier. On September 3, 2015, the clerk accepted for filing a defective document it had no authority to accept.
8. Thus, as of today, January 4, 2016, the State has not properly filed a notice of appeal with the Circuit Court for Baltimore City in this case. Today marks the 123rd day “after the decision [was] rendered.” Accordingly, the instant appeal has not been filed within the time prescribed by rule.

WHEREFORE, Appellee respectfully requests that this Court dismiss the instant appeal pursuant to Maryland Rule 8-602(a)(3) because the notice of appeal was not filed with the lower court within the time prescribed by Maryland Rule 8-202.

Respectfully submitted,



Daniel Kobrin
Assistant Public Defender
Office of the Public Defender
Appellate Division

6 Saint Paul Street, Suite 1302
Baltimore, Maryland 21202-1608
Work: (410) 767-2307
Fax: (410) 333-8801
Dkobrin@opd.state.md.us

Counsel for Appellee

**IN THE
COURT OF SPECIAL APPEALS OF MARYLAND**

SEPTEMBER TERM, 2015

NO. 1496

STATE OF MARYLAND,

Appellant

v.

KERRON ANDREWS,

Appellee

**APPEAL FROM THE CIRCUIT COURT FOR BALTIMORE CITY
(JUDGE KENDRA Y. AUSBY, MOTIONS JUDGE)**

APPELLEE'S BRIEF

STATEMENT OF THE CASE

Appellee adopts the Statement of the Case set forth in Appellant's Brief.

QUESTIONS PRESENTED

1. Can the suppression court's findings of fact be clearly erroneous when they are supported directly by the testimony of the State's witness?
2. Was the suppression court correct in ruling that the BPD's use of a cell site simulator to track the precise location of a cell phone inside of a home constituted a "search" within the meaning of the Fourth Amendment?
3. Was the suppression court correct in ruling that any fruit of that illegal search was inadmissible at Mr. Andrews' trial?

STATEMENT OF FACTS

Appellee adopts the summary of facts underlying the charges in this case set forth by Appellant's Brief. As for the procedural history giving rise to this appeal, Appellee adds the following.

Mr. Andrews' motion to suppress was the product of an arduous discovery dispute that uncovered efforts by law enforcement to withhold exculpatory evidence and hide details of its investigation. The origins of the dispute lay in a November 3, 2014 Supplemental Discovery Request issued by defense counsel in this case. (R. 38). The request, asking for no more than what the State was compelled to disclose pursuant to Maryland Rule 4-263, sought: 1) "records, notes, and documents" relating to the Baltimore Police Department's investigation into a second suspect from the April 27, 2014 shooting; as well as 2) information "indicating how Mr. Andrews was located at 5032 Clifton Avenue." (R. 32).¹

Over two months later, on January 8, 2015, the State responded to the discovery request. The State claimed not to "possess information related to the method used to locate the Defendant at 5032 Clifton Avenue." (T1 9).² This turned out to be false.

¹ The discovery request also specifically asked for "notes, documents, search warrants, location information, and reports" related to the pen register trap and GPS tracking used during the investigation. (R. 32).

² Transcript references are as follows:

"T1" for the May 12, 2015 discovery violations hearing;

"T2" for the May 21, 2015 discovery violations hearing;

"T3" for the June 4, 2015 discovery violations hearing; and,

Between January 8, 2015 and May 6, 2015, Mr. Andrews' trial date was twice postponed for reasons unrelated to this discovery dispute. On May 6, 2015, defense counsel received an email from the Assistant State's Attorney (ASA) assigned to the case informing her that, in fact, a cell site simulator was used by the "ATT [Advanced Technical Team]" squad of the Baltimore Police Department (BPD) to locate Mr. Andrews during its investigation. (T1 10-11; R. 45-46). That fact had been known by members of the BPD since the date of Mr. Andrews' arrest, over a year earlier. The next day, on May 7, 2015, defense counsel received "contents of the ATT file for [Mr. Andrews'] phone number." (T1 11).

Also on May 7, the ASA shared with defense counsel that she had recently concluded an interview with one of the victims in the case. (T1 12). During that interview, the victim "indicate[d] to the [ASA] that there was a negative photo array." *Id.* (Emphasis added). The prosecutor admitted, though, that she did not have the array and "[didn't] know why it hasn't been disclosed." *Id.* The array had been conducted sometime in January 2015. *Id.* Defense counsel received the exculpatory evidence on May 11—four months and two trial dates later. *Id.*

On the trial date set for May 12, 2015, defense counsel moved for dismissal of the case and suppression of evidence due to the State's multiple discovery violations. A hearing on the motion began before Judge Charles J. Peters on that date and continued at two further dates: May 21, 2015 and June 4, 2015. Over the course of the hearings, the State turned over more information regarding the

"T4" for the August 20, 2015 suppression hearing.

BPD's use of a cell site simulator to track and locate Mr. Andrews. (R. 17-18, 41-42, 48, 51-54). Among these mid-May disclosures was a **second** withheld photo array conducted by another eyewitness in which Mr. Andrews was not identified as a shooter,³ the BPD's application for a pen register trap/trace order, and the resultant order used to justify the State's use of cell site simulation surveillance in this case. (T3 93, 96; R. 54-73). All of the documents pertaining to the surveillance pre-dated the defense's November 2014 discovery request.

The discovery hearing did not proceed well for the State. After its conclusion on June 4, 2015, Judge Peters found that the lead investigator into the shooting at issue, Detective Jeffrey Converse, "**intentionally withheld**" multiple pieces of exculpatory evidence. (T3 126, 128) (emphasis added). The withheld evidence included both photo arrays and a set of the BPD's investigatory notes supporting the defense's theory that Mr. Andrews had no motive to effectuate a shooting. (T3 93). As a result, Judge Peters excluded Detective Converse's testimony entirely from trial. (T3 128).

As for the State's failure to disclose timely "[a]ll relevant material or information regarding...specific searches and seizures, eavesdropping, and electronic surveillance including wiretaps," Md. Rule 4-263(d)(7)(A), Judge Peters found that a postponement cured any prejudice that the lack of disclosure imparted on the defense's trial preparation. (T3 126-27). He thus declined to

³ This photo array was conducted in May 2014. (T3 92). It had been withheld for over a year.

dismiss the case and denied the defense's motion to exclude the gun and telephone seized pursuant to the undisclosed investigative techniques. (T3 129). At the same time, Judge Peters understood that the defense's deadline to file a Motion to Suppress based on the constitutional infirmity of BPD's surveillance techniques had passed, *see* Md. Rule 4-252; the judge therefore granted defense counsel leave to file a belated suppression motion. (T3 108).

Defense counsel filed a 56-page Motion to Suppress, including exhibits, on June 30, 2015. (R. 16-72). In the motion, the defense sought suppression of all evidence obtained through the use of the cell site simulator—Hailstorm in this case—as “fruit of the poisonous tree.” (R. 11). In particular, the motion asserted that the use of the cell site simulator constituted a “search” within the ambit of the Fourth Amendment (R. 21-24), that the search was undertaken without a warrant (R. 20); and, that the pen register order obtained by BPD could not authorize the use of a cell site simulator. (R. 26-33).

Thirty days later (outside of the 15-day deadline for filing a response, *see* Md. Rule 4-252(f)), the State filed its response. The State's single assertion: suppression had already been decided by Judge Peters. (T4 6). Defense counsel (and the suppression court) thus walked into the suppression hearing on August 20, 2015, without knowing what arguments the State planned to raise in opposition to the challenge.

ARGUMENT

This case challenges the BPD's use of a cell site simulator, Hailstorm, to track and locate an individual inside of a home. The issue, in particular, is whether such a use of a Hailstorm device constitutes a search under the Fourth Amendment to the United States Constitution; and, if so, whether the BPD's search in this case, conducted pursuant to a state-level pen register order, passes constitutional scrutiny. As of the filing of this brief, Counsel for Appellee has not identified another appellate case of this kind anywhere in the county.

The Hailstorm device in this case functioned by emitting indiscriminately a multi-directional signal into nearby homes, and into the cellular telephones inside of those homes, in order to query the cellular telephone's identifying information. (T3 48-49, 52, 54). The emitted signal "capture[d]" the cellular phone and prompted it to transmit its identifying information back to the Hailstorm device, linking the phone's cellular radio signal to the device. (T3 49, 52-53). With that link established, the Hailstorm device evaluated the cellular signal's strength and direction in order to guide itself to the geographic location of the phone. (T3 50).

The analysis of how that behavior unconstitutionally infringed on Mr. Andrews' Fourth Amendment freedoms proceeds in five parts:⁴

⁴ Appellate review of the suppression ruling proceeds under two standards. This Court pays "great deference" to the first-level factual findings of the suppression court, contradicting them only when they appear clearly erroneous. *Brewer v. State*, 220 Md. App. 89, 99 (2014). Accordingly, all facts and inferences therefrom are viewed in the light most favorable to the prevailing party—Mr.

- First: The suppression court’s factual findings regarding how a Hailstorm operates—sending a signal both into homes and into the phones inside those homes—were not clearly erroneous. They were supported by the record.
- Second: Sending a signal into a home to evaluate the presence of a cellular activity constitutes a search under the Fourth Amendment; and, sending a signal into a cellular telephone to evaluate its identifying information, thereby obtaining its location, constitutes a search and seizure under the Fourth Amendment.
- Third: The third-party doctrine of *Smith v. Maryland*, 442 U.S. 735 (1979) cannot negate the expectations of privacy in one’s home and the contents of one’s cell phone.
- Fourth: The pen register order obtained by BPD in this case was not a quasi-warrant, rendering the use of the Hailstorm constitutionally permissible.
- Fifth: A subsequent search warrant, issued upon facts learned through the use of the Hailstorm device, withers as fruit of the poisonous tree. Good faith is inapplicable.

The suppression court in this case, Judge Kendra Y. Ausby presiding, ruled correctly in this case correctly on all above points (T4 30-31, 36-37, 46, 49). That ruling should be affirmed on appeal.

Andrews. *Id.* At the same time, the legal conclusion of the suppression court is reviewed *de novo*. *Id.*

The State complains that the suppression court “disregarded” appropriate standards in reaching its ruling, asserting that Judge Ausby ought to have deferred to the probable cause determination of a prior judge. (Appellant’s Brief at 6-7). The State’s argument fails basic scrutiny. Judge Ausby was not sitting in a “deferential” review of a neutral magistrate’s probable cause determination. No neutral magistrate had reviewed the search warrant application with the constitutionally-tainted information excised. The suppression court thus conducted a *de novo* review of the search warrant’s sufficiency under the independent source doctrine, a task this Court and the Court of Appeals have done properly on a consistent basis. *See e.g. Holmes v. State*, 368 Md. 506, 517 (2002); *Redmond v. State*, 213 Md. App. 163, 190 (2013).

I. THE SUPPRESSION COURT’S FINDINGS OF FACT WERE SUPPORTED DIRECTLY BY THE TESTIMONY OF THE STATE’S WITNESS.

Prior to its formal ruling, the suppression court made findings of fact about how the Hailstorm device was operated in this case to locate Mr. Andrews. The State condemns those findings, inimical to its entire constitutional argument, as “clearly erroneous” because they are “not supported by anything in this record.” (Appellant’s Brief at 9). In fact, the court’s findings were supported by multiple portions of testimony.

Judge Ausby found, as a matter of fact, that Hailstorm operated by emitting a signal “through the wall of a house” and “into the phone.” (T4 31, 36-37). Once in the phone, the Hailstorm device “gets information out of the phone,” (T4 45), by “forc[ing] the phone to emit that information.” (T4 38). Accordingly, use of the Hailstorm “violat[e]d the Defendant’s Fourth Amendment rights.” (T4 48).

The suppression court’s findings were not clearly erroneous. This Court has explained:

A holding of “clearly erroneous” is a determination, as a matter of law, that, even granting maximum credibility and maximum weight, there was no evidentiary basis whatsoever for the finding of fact. The concern is not with the frailty or improbability of the evidentiary base, but with the bedrock non-existence of an evidentiary base.

It is akin to holding, as a matter of law, that the evidence was not legally sufficient to support a verdict.

State v. Brooks, 148 Md. App. 374, 299 (2002) (emphasis added). In essence, the State must show that Judge Ausby's findings were concocted from thin air, with no evidentiary basis in the record, to declare them clearly erroneous.

The following is the basis from which Judge Ausby found that the Hailstorm device probed "through the wall of a house" and "into the phone," and thereafter "gets information out of the phone."

[Defense Counsel]: Okay. And so, if a person is inside of a home, that equipment [Hailstorm] peers over the wall of the home, to see if that cell phone is located behind the wall of that house, right?

[Det. John Haley, ATT of BPD]: Right.

[Defense Counsel]: **And it sends an electronic transmission through the wall of that house, correct?**

[Det. John Haley, ATT of BPD]: Yes.

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

[Det. John Haley, ATT of BPD]: 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 MSID. And that's like a ten digit—like a ten-digit number. So it's retrieving that. And there's also the electronic serial number. It's retrieving that. And that's really it.

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

[Assistant State's Attorney]: Objection.

[Det. John Haley, ATT of BPD]: **Right.**

THE COURT: Overruled.

[Det. John Haley, ATT of BPD]: Yeah, ma'am. Like I said before, we're—

[Defense Counsel]: I'm sorry, the question was, it's not pinging, right?

[Det. John Haley, ATT of BPD]: I don't understand pinging.

[Defense Counsel]: Pinging means that when a call is made, it will ping to a cell tower, to let you know where the call is coming from. That's not what—

[Assistant State's Attorney]: Objection.

[Defense Counsel]:—happens, right?

THE COURT: Overruled.

[Det. John Haley, ATT of BPD]: 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?

[Det. John Haley, ATT of BPD]: 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?

[Det. John Haley, ATT of BPD]: Well, I would say it does act like a cell tower, because the only time that you're going to connect—the only time 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?

[Det. John Haley, ATT of BPD]: 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?

[Det. John Haley, ATT of BPD]: Okay.

[Defense Counsel]: And you want to know where I am, correct?

[Det. John Haley, ATT of BPD]: Okay.

[Defense Counsel]: Yes?

[Det. John Haley, ATT of BPD]: Yes.

[Defense Counsel]: And you're driving through my neighborhood, right?

[Det. John Haley, ATT of BPD]: Okay.

[Defense Counsel]: Looking for me, correct?

[Det. John Haley, ATT of BPD]: Correct.

[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?**

[Det. John Haley, ATT of BPD]: **Correct.**

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

[Det. John Haley, ATT of BPD]: Correct.

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

[Det. John Haley, ATT of BPD]: Yes.

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

[Det. John Haley, ATT of BPD]: Yes.

(T3 48-49, 50-54). Examining the above testimony and the inferences drawn therefrom in a light most favorable to Mr. Andrews (as this Court must, *Brewer*, 220 Md. App. at 99), Judge Ausby's factual findings cannot be declared clearly erroneous. There is ample, explicit support in the record that a Hailstorm device draws identifying information from a cell phone by transmitting a signal through the walls of a home and into the receiver of a cell phone.

Of course, the State is correct that the above testimony comes from a "summary" source. (Appellant's Brief at 7). That source, Detective Haley, was forbidden by signed memorandum between the BPD, Baltimore City State's Attorney's Office, and FBI, from "distribut[ing], disseminat[ing], or otherwise disclos[ing] any information concerning the wireless collection equipment/technology or any software, operating manuals, or any technical documentation . . . to the public, including to any non-law enforcement individuals or agencies." (Apx. 2). That source is also an agent of an organization that cloaked itself in international arms control law to avoid disclosing how a Hailstorm works. (Apx. 7-8). To say the least, members of the Baltimore Police Department have not been forthcoming in explaining accurately how a Hailstorm works. Nonetheless, Detective Haley described accurately how invasive a Hailstorm search can be.

Hailstorm is an **active**⁵ cellular surveillance device that works by “impersonating a wireless base transceiver station... and tricking the target’s phone into connecting to it.” Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harvard J. Law & Tech. 1, 11 (2014).⁶ The Hailstorm in this case was used to find a particular phone; the device, however, is capable of identifying all nearby phones in a certain geographic vicinity and intercepting substantive communications sent by a phone. *Id.* Critical to the instant appeal, active surveillance devices, like Hailstorm, “send signals, often indiscriminately, through the walls of homes, vehicles, purses, and pockets in order to probe and identify the phones located inside.” *Id.* at 12 (footnotes omitted). When its signal reaches the target phone, that phone is effectively “tricked” into sending back its unique serial number or other identifying data. Stephanie K. Pell & Christopher Soghoian, *A Lot*

⁵ A passive device is what the State mistakenly describes in its brief: “Passive wireless surveillance devices do not transmit any signals. These devices are thus far more covert in operation—indeed effectively invisible—but they can only detect signals of nearby phones when those phones are actually transmitting data.” Pell, *supra* at 13. Detective Haley confirmed that his Hailstorm device was not passive when he explained that it would not operate on a phone that was actively transmitting data. (T3 51-52).

⁶ The cited article describes the operation of an active cell site simulation device called “Stingray.” It explains that Hailstorm is merely an upgraded version of Stingray, able to operate with phones connected to higher-speed, 4G networks. Pell, *supra* at 70-71. Hailstorm is to Stingray what an iPhone 6 is to a flip-phone.

More than a Pen Register, and Less than a Wiretap, 16 Yale J. Law & Tech 134, 145 (2013).

This Court may rest assured that Judge Ausby’s findings of fact were not clearly erroneous. Those findings rested upon ample testimony in the record. In turn, that testimony (though constrained) accurately portrayed how a Hailstorm device functions. This Court may therefore proceed in its Fourth Amendment analysis with the understanding that Hailstorm operates by transmitting a signal “through the wall of a house” and “into the phone,” (T4 31, 36-37); and, once in the phone, the Hailstorm device “gets information out of the phone.” (T4 45).

II. THE SUPPRESSION COURT CORRECTLY RULED THAT THE USE OF A CELL SITE SIMULATOR TO TRACK THE PRECISE LOCATION OF A CELL PHONE CONSTITUTED A “SEARCH” WITHIN THE MEANING OF THE FOURTH AMENDMENT.

The Fourth Amendment to the United States Constitution protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const., amend. IV.⁷ “[T]he most basic constitutional rule in this area is that ‘searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment.’” *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971); accord *Spence v. State*, 444 Md. 1, 6 (2015). The warrant requirement ensures that a “neutral and detached magistrate” scrutinizes the circumstances supporting an invasion of privacy, rather than “the officer engaged in the often

⁷ Made applicable to the States through the Fourteenth Amendment. *Mapp v. Ohio*, 367 U.S. 463, 660 (1961).

competitive enterprise of ferreting out crime.” *Riley v. California*, 134 S.Ct. 2473, 2482 (2014) (quotation omitted).

A “search,” requiring a warrant under the Fourth Amendment, occurs when the State invades a subjective expectation of privacy that society recognizes as reasonable. *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). A subjective expectation of privacy is present when an individual seeks to preserve a matter as private. *Williamson v. State*, 413 Md. 521, 535 (2010). That expectation is deemed reasonable by society when it stems from, “concepts of real or personal property law or... understandings that are recognized and permitted by society.” *Minnesota v. Carter*, 525 U.S. 83, 88 (1998).

In this case, the State contravened two subjective, reasonable expectations of privacy. Mr. Andrews’ expectation that the government would not “determine by means of an electronic device ... whether a particular article—or person, for the matter—is in an individual’s home at a particular time,” *United States v. Karo*, 468 U.S. 705, 716 (1984) and, the expectation one has in the contents of a personal cell phone, including location data, *see Riley*, 134 S.Ct. at 2490; *see also Tracey v. State*, 152 So.3d 504, 525-26 (Fla. 2014).

**A. Use of a Hailstorm to evaluate cellular activity
inside of a home is a search.**

The amendment itself lists four areas in which a person possesses a categorical expectation of privacy: “persons, houses, papers, and effects.” U.S.

Const., amend IV; *see Oliver v. United States*, 466 U.S. 170, 176 (1984). Of the four, though, “the home is the first among equals.” *Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013). The Fourth Amendment applies with the greatest force inside of the home because that space has been regarded for centuries as the most private. *Georgia v. Randolph*, 547 U.S. 103, 115 (2006). After all, at the core of the amendment “stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.” *Silverman v. United States*, 365 U.S. 505, 511 (1961).

The Fourth Amendment therefore guards closely the boundaries of a home, “draw[ing] a firm line at the entrance to the house.” *Payton v. New York*, 445 U.S. 573, 590 (1980). Invasion “by even a fraction of an inch” constitutes a search that must be supported by a warrant. *Silverman*, 365 U.S. at 512. No detail is too small—“*all* details are intimate details, because the entire area is held safe from prying government eyes.” *Kyllo*, 533 U.S. at 37-38 (emphasis in original). **The State thus engages in a search anytime it surveilles a detail inside a home that it could not have otherwise learned without physical intrusion.** *Id.* at 34; *Karo*, 468 U.S. at 715; *see also Fitzgerald v. State*, 384 Md. 484, 498 (2004).

The use of technology does not transform a search of a home into an unprotected event. To be sure, advancing technology may affect “the degree of privacy secured to citizens by the Fourth Amendment.” *Kyllo*, 533 U.S. at 33-34. That advance, though, does nothing to erode the privacy interest rooted in the home. Though technology may make the invasion of a home less physically

intrusive, it still accomplishes the same evil against which the Fourth Amendment protects: “reveal[ing] a critical fact about the interior of the premises that the government is extremely interested in knowing and that it could not have otherwise obtained without a warrant.” *Karo*, 468 U.S. at 715. Thus, as technology advances to enable less-conspicuous surveillance, “the protections of the Fourth Amendment are ‘more, not less, important.’” *Tracy*, 152 So.3d at 412 (quoting *Coolidge*, 403 U.S. at 455).

In *United States v. Karo* and *Kyllo v. United States*, the Supreme Court demarcated a bright line rule “governing the use of technology to learn the contents of residences.” *Fitzgerald*, 384 Md. at 498. “[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without ‘physical intrusion into a constitutionally protected area,’ constitutes a search.” *Kyllo*, 533 U.S. at 34 (quoting *Silverman*, 365 U.S. at 512) (emphasis added).⁸ Included within “any information” is confirmation that “a particular article—or a person...—is in an individual’s house at a particular time.” *Karo*, 468 U.S. at 716. Thus, surreptitious surveillance technology that probes the presence of cellular activity in a home is a search under the Fourth Amendment.

⁸ The Supreme Court added: “at least where (as here) the technology in question is not in general public use.” *Kyllo*, 533 U.S. at 34. There is no question here that Hailstorm, a closely-guarded investigative technology that requires FBI approval before it may be purchased, is not “in general public use.”

United States v. Karo illustrates perfectly how the circumstances of this case amount to a search. *Karo* was one of two “beeper cases,” in which the Supreme Court determined whether the tracking of a beeper device secreted inside a drum of chemicals constituted a search under the Fourth Amendment. In the first beeper case, *United States v. Knotts*, 460 U.S. 276 (1983), law enforcement officers monitored a wireless radio transmitter installed in a container of chloroform to track the movements of an automobile carrying the container. *Id.* at 278-79. The Supreme Court held that electronic surveillance of the automobile’s journey did not constitute a search. *Id.* at 285.

To reach that holding, the Court relied heavily on the “diminished expectation of privacy in a motor vehicle,” *id.* at 281, and the limitation of the surveillance to tracking movement on a public road, at 282. Because movements on a public road were exposed to the general public, there could be no expectation of privacy in a public journey. *Id.* Thus, the electronic surveillance of the vehicle travelling on a public highway escaped Fourth Amendment scrutiny.

In *Karo*, law enforcement officers used identical surveillance technology to confirm the presence of a drum of ether inside of suspect’s home. 468 U.S. at 708. Distinguishing the case from *Knotts*, the Supreme Court, “[a]t the risk of belaboring the obvious,” pointed out that homes and highways do not occupy the same protected space under the Fourth Amendment. *Id.* at 714. While an automobile on a highway was exposed to public observation, “private residences [were] places in which the individual normally expects privacy free of

governmental intrusion not authorized by a warrant.” *Id.* at 714. The fact that the surveillance peered inside of a home, rather than inside of a car on a public highway, fundamentally altered the issue at hand.

The Supreme Court in *Karo* explained that the use of the electronic monitoring to confirm the presence of the container revealed a “critical fact about the interior of the premises.” *Id.* at 715. That fact was, “that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched.” *Id.* Because that fact could not otherwise be verified by visual observation, its divination constituted an intrusion into a constitutionally protected place. *Id.* at 715-16. The Supreme Court therefore concluded that the wireless surveillance of the beeper device, which resulted in learning a detail about the interior of a home, constituted a search under the Fourth Amendment. *Id.* at 716.

Kyllo v. United States followed directly in the footsteps of *Karo*, reinforcing the notion that extra-sensory surveillance of in-home activity constituted a search under the Fourth Amendment. 553 U.S. at 36-38. In *Kyllo*, law enforcement officers used a thermal-imaging device to observe “that Kyllo’s garage roof and side wall were relatively hot compared to the rest of his home.” *Id.* at 30. The thermal picture obtained by the officers reinforced their suspicion that Kyllo had been using heat lamps to grow marijuana inside his home. *Id.* The Supreme Court held that use of the thermal-imaging device to learn about the heat within the home constituted a search under the Fourth Amendment. *Id.* at 40.

The Supreme Court reasoned that a bright line separated the interior of the home from the rest of the world. *Id.* at 33-34, 40. It did not matter whether the State crossed that line by physical intrusion or sense-enhancing surveillance—the crossing of the line constituted the search. *Id.* at 34. Once the government learned of a detail, any detail, about the interior of the home, the government had violated a constitutionally-protected zone. *Id.* at 37-38.

The Court also rejected the argument that heat, emanating from the exterior of the home, was not a detail in which a person manifested a reasonable expectation of privacy. “The Fourth Amendment’s protection of the home has never been tied to the measurement of the quality or quantity of information obtained.” *Id.* at 37. The *Kyllo* Court declared that “all details” regarding the interior of the home were “intimate details” because they revealed something about the most-protected space in American jurisprudence. *Id.* at 37-38. The *Kyllo* Court also adopted a “long view” of Fourth Amendment protection—in *Kyllo* the government observed the heat signature of the home; in a future case it might observe a visual image of the contents of the home. The Fourth Amendment thus acted as a shield against technological creep that, in the future, could pry further into the privacy of the home. *Id.* at 40 (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)).

Karo, *Kyllo*, and the Fourth Amendment barrier at the entrance of the home compel only one conclusion in this case: the use of a Hailstorm to probe the presence of cellular activity in a home constitutes a search under the Fourth

Amendment. The circumstances of Mr. Andrews' case are no different than the circumstances of *Karo*. There, law enforcement officers used wireless surveillance technology to determine the geographic location of a can of ether inside of a home. Here, law enforcement officers used wireless surveillance technology to determine the geographic location of a cell phone inside of a home. In *Karo*, the monitoring of the beeper, revealing its location, constituted a search because it revealed that "a particular article [was] actually located at a particular time in the private residence...." 468 U.S. at 715. Here, the use of the Hailstorm device, "captur[ing]" a cell phone signal and revealing the cell phone's location, constituted a search because it revealed that the cell phone was actually located inside 5032 Clifton Avenue on May 5, 2014.

The State attempts to distinguish *Karo* and *Kyllo* from the instant case by differentiating between private property withdrawn from public view and a cell phone, which emits identifying information to nearby cell phone towers. (Appellant's Brief at 11-12). Because the former is ostensibly hidden within a home, its discovery constitutes a search; the latter is not similarly hidden because it constantly transmits information. (Appellant's Brief at 12). The State's distinction is one without substance, though, in two respects.

First—discussed in greater detail below, *see infra* Arg. II.C.—the notion that a cell phone identifying with a nearby tower is equivalent with sharing real-time, pinpoint location data with law enforcement is wrong. A cell phone user does not "voluntarily" share his or her exact location data with a cell phone tower,

as that term is used in *Smith v. Maryland*. Moreover, cell site location information (the information gleaned from the constant phone-to-tower check-ins) is nowhere near as geographically precise as what a Hailstorm can achieve by capturing a single phone. In any event, the existence of cell towers and stored location data is irrelevant, as the Supreme Court explained:

The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment. The police might, for example, learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful.

Kyllo, 533 U.S. at 35 n. 2.

Second—and more pertinent to the doctrine at issue—the Supreme Court in *Kyllo* made painfully clear that the object of the unlawful surveillance need not be private property withdrawn from view. “[A]ll details” gleaned about the interior of the home are “intimate details.” 533 U.S. at 37-38. Heat emanating from a portion of the roof revealed the relative temperature of the underlying room. *Id.* at 38. There is nothing inherently private about heat, but such a focus misses the point. Because the temperature of the home could not be learned without an officer walking into the home with a thermometer, the learning of that information by sense-enhancing technology was a search. *Id.* at 40.

The same is true in this case. A cell phone signal transmitted from within a home was “capture[d]” by the BPD’s Hailstorm device. Following the directional dynamic of that transmission, officers learned that the cell phone was located

inside 5032 Clifton Avenue. That fact could not have been learned without the officers walking into the home and rifling through every crevice that could contain a cell phone. “Where, as here, the Government use[d] a device that is not in general public use, to explore details of a home that would previously have been unknowable without physical intrusion, the surveillance [was] a ‘search’ and is presumptively unreasonable without a warrant.” *Id.* at 40.

B. Use of a Hailstorm to wirelessly capture location information from a cell phone is a search and seizure.

The breadth and depth of personal information contained in a modern cell phone is staggering. From personal correspondence to pinpoint location data, a cell phone acts as a repository for nearly any-and-every intimate detail of an individual’s life. *Riley*, 134 S.Ct. at 2495. Thus, the intrusion into the home constituted only the first search effectuated by BPD’s use of the Hailstorm device in this case. By transmitting a signal “into [Mr. Andrews’] phone,” “get[ting] information out of the phone,” and “forc[ing] the phone to emit that information,” (T4 31, 36-38, 45, 48), the Hailstorm device contravened Mr. Andrews’ reasonable expectation of privacy in his cell phone. *See Riley*, 134 S. Ct. at 2494-95; *see also Tracy*, 152 So. 3d at 526. That second search, undertaken without a warrant, further requires this Court to affirm Judge Ausby’s suppression ruling.

The Supreme Court recently explicated the privacy interests at stake with cell phone technology in *Riley v. California*, 134 S.Ct. 2473 (2014). In that case, the Court confronted whether law enforcement officers may search the contents of

a cell phone incident to a lawful arrest. *Id.* at 2480. After balancing the government’s interests in officer safety and preservation of evidence against an individual’s privacy interest in the contents of a cell phone, the Court declined to extend the search-incident-to-arrest exception to the search of a cell phone’s digital content. Instead, “officers must generally secure a warrant before conducting such a search.” *Id.* at 2485.

Arriving at that disposition required the *Riley* Court to scrutinize the degree of privacy a modern American cell phone user expects in the contents of his or her phone. *Id.* at 2484. The Court began that task by noting how 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.” *Id.* The *Riley* Court then measured how cell phones “differ in both a quantitative and a qualitative sense” from other objects an individual normally carries. *Id.* at 2489.

Quantitatively, a modern cell phone acts as an immense storage locker for a wide range of personal data. *Id.* Addresses, notes, prescriptions, bank statements, text messages, calendar entries, photos, and videos might all be found within the contents of a cell phone. *Id.* Moreover, a cell phone holds hundreds, or even thousands, of each of the above given the growing storage capacity of modern devices. *Id.* at 2489-90. In that sense, modern cell phones are closer kin to “minicomputers” than a “wallet, or purse.” *Id.* at 2488-89.

Qualitatively, modern cell phones permit the collection and aggregation of data heretofore unknowable to curious outsiders—including location data. *Id.* at

2490-91. Internet searches and browsing histories are stored in a phone's memory. *Id.* at 2490. This allows record-creation of a person's "interests or concerns." *Id.* Critical to this case, "[d]ata on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* (citing *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring)). Accordingly, a cell phone search may be more invasive than the search of a home because a cell phone contains data—such as location information—“never found in a home in any form.” *Id.* at 2491.

Given the quantitative and qualitative differences, the Supreme Court in *Riley* concluded that cell phones contain “the privacies of life.” *Id.* at 2495 (citing *Boyd v. United States*, 116 U.S. 616, 630 (1967)). As a result, cell phones deserved Fourth Amendment protection from the prying eyes of government investigators. *Id.* The “answer to the question of what police must do before searching a cell phone seized incident to arrest” was plain: “get a warrant.” *Id.*

If law enforcement officers must obtain a warrant to search a cell phone incident to the arrest of its user, *a fortiori* those officers must obtain a warrant to search the digital content of a cell phone without its user's knowledge. The *Riley* Court's analysis dictates that a cell phone user maintains a reasonable expectation of privacy in the contents of a cell phone because the phone contains incredibly sensitive information, including location data. *Tracy*, 152 So.3d at 524; *see also*

United States v. Graham, 796 F.3d 332, 349-50 (4th Cir. 2015) rehearing en banc granted at 2015 WL 6531272 (Oct. 28, 2015); *In re Application of the United States for an Order Authorizing Disclosure of Location Information for a Specified Wireless Telephone*, 849 F.Supp.2d 526, 541-42 (D. Md. 2011). With that in mind, two appellate courts have held that obtaining real-time location data from a cell phone constitutes a search under the Fourth Amendment.

In *Tracey v. State*, 152 So.3d 504 (Fla. 2014), the Supreme Court of Florida decided whether the gathering of real-time cell site location information (CSLI)⁹ constituted a Fourth Amendment search. *Id.* at 511. The Court’s analysis consisted of surveying applicable Supreme Court precedent, including *Karo*, *Kyllo*, and *Riley*, *id.* at 512-15, and a “normative inquiry,” analyzing how citizens should view locational privacy given the ubiquity of tracking. *Id.* at 519-26. The *Tracey* Court’s conclusion: “[T]he use of [the Petitioner’s] cell site location information emanating from his cell phone in order to track him in real time was a search within the purview of the Fourth Amendment for which probable cause was required.” *Id.* at 526.

Pertinent here, the Supreme Court of Florida’s “normative analysis” highlighted the importance of privacy in location data. That analysis began with

⁹ “Cell site location information (also referred to as CSLI) refers to location information generated when a cell phone call occurs.... The location of the cell phone can be pinpointed with varying degrees of accuracy depending on the size of the geographic area served by each cell tower, and is determined by reference to data generated by cell sites pertaining to a specific cell phone.” *Tracey*, 152 So.3d at 507, n. 1.

the Tracey Court's approval of Justice Sonia Sotomayor's concurrence in *United States v. Jones*, which outlined the immense concerns attached to government-based location tracking. 132 S.Ct. 945, 955-56 (2012) (Sotomayor, J., concurring). Chief among those concerns was the potential creation of a "comprehensive record of a person's public movements," which could "alter the relationship between citizen and government in a way that is inimical to democratic society"; namely, "[a]wareness that the Government may be watching chills associational and expressive freedoms." *Tracey*, 152 So.3d at 519-20 (quoting *Jones*, 132 S.Ct. at 955-56). Given that concern, it was unwise to trust the executive branch to self-police its use of tracking technology "in light of the Fourth Amendment's goal to curb arbitrary exercises of police power and prevent a too permeating police surveillance." *Id.* at 521 (quoting *Jones*, 132 S.Ct. at 956). The Fourth Amendment, and the warrant requirement in particular, were the balancing point between the immense power of location tracking technology and the police's competitive desire to use it. *Id.*

The *Tracey* Court also noted that the third-party doctrine (discussed below, *infra* Arg. II.C) fit poorly in the modern context of location information. "The fiction that a 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." *Id.* at 523 (quotation omitted). Cell phones are simply too ubiquitous in the personal, everyday lives of most Americans for their locational transmissions to be considered a voluntary choice.

Id. at 524-25 (citing *Riley*, 134 S.Ct. 2489). “[O]wners of cell phones...do not contemplate that the devices will be used to enable covert surveillance of their movements.” *Id.* at 524. It was thus proper to view cell phones as an “effect,” as that term is used in the Fourth Amendment, and bestow upon them the same constitutional privacy protection as a sealed package or personal luggage. *Id.* at 525 n. 15.

Based on its analysis, the *Tracey* Court concluded that a cell phone user maintains a “subjective expectation of privacy in the location signals transmitted solely to enable private and personal use of [a] cell phone.” *Id.* at 525. Moreover, that expectation was one “society is now prepared to recognize as objectively reasonable.” *Id.* at 526. The real-time tracking of cell site location information emanating from a cell phone, and through a cell tower, constituted a search under the Fourth Amendment. *Id.*

United States v. Graham, 796 F.3d 332 (4th Cir. 2015) applies the same analysis and reaches an identical result.

The same must be true in this case. Mr. Andrews possessed a cell phone. That cell phone contained “the privacies of [his] life.” *Riley*, 134 S. Ct. 2495. Among those privacies was his precise location information, both in a historical aggregate and at any given moment in real time. Given the intimate nature of that information, *Jones*, 132 S.Ct. at 955-56, Mr. Andrews maintained an expectation of privacy in the digital integrity of his cell phone. *Tracey*, 152 So.3d 526; *Graham*, 796 F.3d at 360-61. And that expectation must be judged reasonable. *Id.*

The Fourth Amendment must apply to protect the digital information stored within Mr. Andrews' cell phone. *Riley*, 134 S.Ct. at 2495.

The BPD thus initiated a warrantless search the moment it withdrew digital information from Mr. Andrews' phone. To be sure, as the State asserted, the Hailstorm device probed only identifying information within the phone. (Appellant's Brief at 8 n.4). That information, however, acted as a proxy; the identifying information drawn from Mr. Andrews' phone functioned as a locational marker for the Hailstorm device, permitting law enforcement officers to figure out the exact location of Mr. Andrews' phone. The BPD essentially queried the phone: "where are you?" It then measured the strength and direction of the phone's response: "I'm here!" (T3 50). Like a game of wireless Marco-Polo, the Hailstorm device used the identification information "capture[d]" from the phone as an inferential tether. The identification information was, functionally, the location information. See Pell & Soghian, *A Lot More than a Pen Register*, *supra* at 145-46. The wireless drawing of that location information from within the phone constituted a search under the Fourth Amendment. *Tracey*, 152 So.3d 526; *Graham*, 796 F.3d at 360-61.

It is worth further noting that the Hailstorm's creation of a wireless tether, "captur[ing]" the cell phone and "forc[ing] the phone to emit [identification] information." (T4 38), also constituted a seizure under the Fourth Amendment. Traditionally, a Fourth Amendment seizure of an article or effect takes place when "there is some meaningful interference with an individual's possessory interests in

that property.” *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Beyond that, the Supreme Court has commented that a conversation is seized when law enforcement officers eavesdrop on a wiretapped telephone line. *Berger v. New York*, 388 U.S. 41, 59 (1967); *see also LeClair v. Hart*, 800 F.2d 692, 695 (7th Cir. 1986) (and cases cited therein) (identifying information, such as serial numbers and titles, are “seized” under Fourth Amendment when copied down or documented by law enforcement).

There can be little doubt, then, that the Hailstorm device seized Mr. Andrews’ phone when it captured the phone’s signal and linked itself to that signal. (T3 49, 52-53). Detective Haley’s testimony made clear that the Hailstorm ripped the cell phone’s signal from the tower to which it had been connected; and, attached that signal to itself for the purpose of tracking the phone. (T3 51). Removing the signal from a cell tower “interfered with [Mr. Andrews’] possessory interest” in his cellular signal and cell phone. *Jacobsen*, 466 U.S. at 113. The phone’s connection with the cell tower allowed Mr. Andrews to maintain his ability to communicate with the broader cellular network (and its users), as well as established a record for his account’s “billing, coverage, and analytics purposes.” *State v. Payne*, 440 Md. 680, 695 (2014).

The State therefore seized and searched Mr. Andrews’ phone when it activated Hailstorm, transmitted a signal “into the phone,” (T4 31, 36-37), “[g]o[ut] information out of the phone,” (T4 45), and, through that information, linked itself to the phone to locate it. (T3 50). The Hailstorm device usurped the cellular signal

of the phone and used that signal to withdraw locational data from within the phone's digital confines. By violating Mr. Andrews' reasonable expectation of privacy in the contents of his cell phone, the BPD engaged in two Fourth Amendment actions that required a warrant. The BPD's failure to obtain a search and seizure warrant for the phone renders those actions unconstitutional.

C. The third-party doctrine cannot excuse the BPD's searches in this case.

The State uses the third-party doctrine of *Smith v. Maryland*, 442 U.S. 735 (1979) to argue that use of a Hailstorm can never constitute a search.¹⁰ The argument is wrong, misinterpreting both the law of the third-party doctrine and the nature of what a cell phone shares with a cell tower. A cell phone user takes no conscious, voluntary action to constantly share location information with a third party. And, the location information gleaned from a cell phone tower is not as precise as that gleaned from a Hailstorm. *Smith* is inapposite.

As an initial point, the State's third-party argument seems only to address whether the intrusion into the phone constituted a search. It is not responsive to

¹⁰ In so doing, the State relies heavily on one of the creakiest doctrines in Fourth Amendment jurisprudence. Commentators have described the *Smith* holding as "the *Lochner* of search and seizure law." Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 563 (2009). The foremost treatise on search-and-seizure jurisprudence criticizes the *Smith* case: "Such a crabbed interpretation of the *Katz* test makes a mockery of the Fourth Amendment." Wayne R. Lafave, 1 *Search and Seizure: A Treatise on the Fourth Amendment*, §2.7(b) (5th ed. West Updated October 2015) (and cases cited therein). The doctrine's viability in a digital age has even been questioned in the highest court in the land: "[The third-party doctrine] is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 132 S.Ct. at 957 (Sotomayor, J., concurring).

whether the intrusion into the home separately constituted a search. The *Smith* opinion made clear that its holding stemmed from the fact that no intrusion into the home was claimed: “Since the pen register was installed on telephone company property at the telephone company’s central offices, petitioner obviously cannot claim that his ‘property’ was invaded or that police intruded into a ‘constitutionally protected area.’” 442 U.S. at 741. Under *Karo*, *Kyllo*, and the cases cited *supra*, Mr. Andrews does so claim—the BPD wirelessly surveilled, and therefore intruded, within a “constitutionally protected area.” *Smith* is wholly inapplicable to the BPD’s use of Hailstorm to “obtain[] by sense-enhancing technology... information regarding the interior of the home that could not otherwise have been obtained without ‘physical intrusion into a constitutionally protected area.’” *Kyllo*, 533 U.S. at 34 (quoting *Silverman*, 365 U.S. at 512).

The third-party doctrine is similarly inapplicable to the search of Mr. Andrews’ phone. The Supreme Court in *Smith* held that an individual maintains no subjective, reasonable expectation of privacy in dialed telephone numbers because that individual voluntarily conveys those numbers to a third-party—the telephone company. 442 U.S. at 745. As a result, the installation of a pen register on telephone company property, which recorded the dialed numbers, did not constitute a search under the Fourth Amendment. *Id.* at 746.

The *Smith* Court arrived at its holding using very specific line of factual and legal reasoning. It pointed out that telephone subscribers “realize” that they send dialed numbers to the telephone company, because without those numbers

the company could not connect calls. *Id.* at 742. Moreover, subscribers “realize” that the dialed numbers are recorded by the telephone company because the subscribers receive a list of phone calls made “on their monthly bills.” *Id.* A telephone subscriber could not, therefore, maintain a subjective expectation of privacy in dialed telephone numbers; the subscriber regularly exposed those numbers to the scrutiny of others. *Id.* at 743.

The *Smith* Court added that, even if an individual established a subjective expectation of privacy in dialed numbers, that expectation was not reasonable. *Id.* The Court’s basis: “a person has no legitimate expectation of privacy in information **he voluntarily turns over to third parties.**” *Id.* at 743-44 (emphasis added). In support the Court cited to its line of informant cases, in which no reasonable expectation of privacy was found in information spoken by the defendant to another person. *Id.* at 744. Buttressing that point, the *Smith* Court asserted that dialing a phone number into the company’s switching equipment was no different than speaking the numbers to a live operator; and, speaking the numbers to a live operator would certainly bring the case within the direct purview of the informant cases. *Id.* at 744-45. Thus, a subscriber who chose to dial numbers into a telephone company’s switching equipment “assume[d] the risk” that the company “would reveal to the police the numbers he dialed.” *Id.* at 744.

A cell phone user does not similarly choose to reveal his or her exact geographic location with a wireless service provider. A cell phone’s periodic contact with a cell tower, disclosing the area in which the cell phone is located, “is

purely a function and product of cellular telephone technology, created by the provider's system network at the time that a cellular telephone call connects.” *Commonwealth v. Augustine*, 4 N.E.3d 846, 862 (Mass. 2014). Unlike dialed numbers, a cell phone user does not actively input location data into the cellular service provider’s system—that data is a by-product, “quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the target user.” *Graham*, 796 F.3d at 355 (quotation omitted). There is no bill at the end of the month informing the cell phone user of all the instances he or she shared location data. There is no informant/operator analogy for a cell phone’s transmission of location data to a tower **because the user does not convey the data, only the phone does**. A cell phone user simply cannot “voluntarily,” *Smith*, 442 U.S. at 743 (emphasis added), convey location information when that information is transmitted by automated electronic compulsion beneath the user’s notice.

Accordingly, a number of courts have declined to apply the *Smith* third-party doctrine to a cell phone’s automated transmission of location information to a tower. *Graham*, 796 F.3d at 355; *In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304, 317 (3d Cir. 2010); *Tracey*, 152 So.3d at 523; *Augustine*, 4 N.E. 3d 862-63; *State v. Earls*, 70 A.3d 630, 641-42 (N.J. 2013).

Of course, the State argues that “[a]nyone who has ever used a smartphone is aware that the phone broadcasts its position on the map.” (Appellant’s Brief at

12). The State fails to support this incredibly broad assertion; nevertheless, the State argues accordingly that the very act of possessing a phone imputes knowledge of its transmissions, rendering voluntary all of its automated location disclosures. (Appellant's Brief at 13-14). The State would essentially have citizens forego technological innovation in order to maintain constitutional privacy rights; throw away cell phones to keep location data private. This Court must reject such a "Luddite approach" to the Fourth Amendment. *King v. State*, 425 Md. 550, 612 (2012) (Barbera, J., dissenting).

Cell phones are more than technological toys that an individual uses at their leisure. As of January 2014, 90% of American adults owned a cell phone. Pew Research Center (Pew Report), *Mobile Technology Fact Sheet*, <http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/> (last accessed December 29, 2015). As of May 2013, 81% of adults used a cell phone to communicate by text message; 60% used a cell phone to access the internet; and 52% use a cell phone to send and receive email. *Id.* It is no mistake to say, then, that "for an increasing portion of our society, [cell phone use] has become essential to full cultural and economic participation." *Graham*, 796 F.3d at 355-56 (citations omitted). Cellular communication, by voice call, text message, and social media participation, has become a keystone instrument of "self-expression" and "self-identification." *City of Ontario, Cal v. Quon*, 560 U.S. 746, 760 (2010).

A cell phone is therefore "essential" in today's society. *Tracey*, 152 So.3d at 523. The cell phone's ubiquity, though, has not eroded privacy attitudes: 82% of

adults report that the details of their physical location revealed through their cell phone's GPS was "somewhat sensitive." Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* at 34, Nov. 12, 2014, http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (last accessed December 29, 2015). Half of adults considered the same information "very sensitive." *Id.*

It would pervert the existence of the Fourth Amendment to hold that an individual, by way of the third party doctrine, must forfeit the right to be free from governmental location tracking in order to obtain a social necessity. An individual does not voluntarily share location data with a third party by happening to own an instrument of communication. "The fiction that a 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." *Tracey*, 152 So.3d at 523. *Smith v. Maryland* cannot apply to this case as a matter of law.

On top of that, *Smith v. Maryland* does not apply as a matter of fact. The State briefly, and without support, asserts that a cell phone "broadcasts its position on the map." (Appellant's Brief at 12). Seemingly, the State attempts to equate the precision of the information derived from Hailstorm with the precision of the information derived from a cell phone's communications with a cell tower. The two are not the same.

Helpfully, the Court of Appeals in *State v. Payne*, detailed exactly how location information may be mined from cell-to-tower transmissions:

A cell phone is, effectively, a sophisticated two-way radio that operates within a cellular network. A cellular network is a wireless network added to the Plain Old Telephone System (POTS), which is the regular, wired form of telecommunications. In order to add a cellular network to the POTS network, equipment is added to the existing telecommunications system. One piece of that equipment is the cell tower and its attached antennae, which is itself one component of a cell site. It is through the cell tower that a cell phone maintains a connection to the telecommunications network.

Cellular networks are comprised of a distribution of land areas called “cells”, each of which is served by at least one cell tower. The arrangement of cells “is based on the concept of dividing the landscape into coverage cells typically three miles in diameter”; therefore, the term “cell” refers to a defined geographic region. These cells are “arranged in the pattern of a hexagonal grid or honeycomb.” A cellular network is designed so that the cells overlap, and the cell tower lies where the several cells intersect, not at the center of a cell. **The coverage of a particular cell may range from one-half mile, particularly in the urban environment, to as far as thirty miles from the cell tower.**

440 Md. at 692-93 (citations omitted) (emphasis added). The U.S. Court of Appeals for the Fourth Circuit provided a similar, helpful explanation. See *Graham*, 796 F.3d at 343 (“The precision of this location data depends on the size of the identified cell sites’ geographical coverage ranges. Cell sites in urban areas, which have the greatest density of cell sites, tend to have smaller radii of operability than those in rural areas.”); accord *Tracey*, 152 So.3d at 507 n.1.

Needless to say, the location data derived from a cell phone's transmission to a nearby cell tower is not geographically precise. Information gleaned from a phone "sharing" with a cell tower can give law enforcement officers a general idea of the area within which to look, but not a precise address or street corner. This is especially true within urban environments, where a cell phone might be transmitting from a multi-story building. In a sense, data derived from tower transmissions can give officers a metaphorical zip code, but not a street address.

Hailstorm provides a street address, metaphorically and literally. As Detective Haley confirmed, the device could pinpoint a phone's location within 20 yards. (T3 51). Use of the Hailstorm device permitted the BPD to isolate the exact residence from which Mr. Andrews' phone had been transmitting. (T3 56-57). This was possible, even though the residence was one of "30-35" attached units arrayed in a "U" shape. (T3 57). Officers were not able to get such precision from the cell tower information they had obtained—they only used the Hailstorm to arrive at an exact location after using cell tower information to locate the correct neighborhood. (T3 78; Appellant's Brief at 3).

It is safe to say, then, that location data from a Hailstorm is substantially more precise than location data from automated transmission shared with a cell tower. The former may lead officers directly to the target phone, the latter can lead them only to its general area. A cell phone therefore does not already share what the police may obtain from a Hailstorm. Through the limits of cell tower

technology, a cell phone cannot share its exact geographic location. To obtain that, the BPD had to take extra measures—a search with a Hailstorm device.

This Court must not hold that *Smith*, and the third-party doctrine, invalidate the searches in this case.

D. A Maryland pen register trap/trace order is not warrant; the order in this case cannot authorize a Fourth Amendment search.

For brevity and ease of reading, the following chart illustrates why a pen register order cannot operate as a warrant to authorize a Fourth Amendment search:

| Search Warrant (Fourth Amendment) | Pen Register Order (Cts. & Jud. Proc. §10-4B-01) |
|---|---|
| Renders “reasonable” an intrusion on a subjective, reasonable expectation of privacy. U.S. Const., amend IV; <i>Katz v. United States</i> , 389 U.S. 347 (1967). | Permits recording or identifying “dialing, routing, addressing, or signaling information,” or source thereof. §10-4B-01(a)&(c). |
| Issues on demonstration of probable cause, that a “fair probability that contraband or evidence of a crime will be found in a particular place.” <i>Illinois v. Gates</i> , 462 U.S. 213, 238 (1983). | Issues on showing “that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation.” § 10-4B-04(a)(1). |
| Finding of probable cause must be attached to a particular suspected crime. <i>Berger</i> , 388 U.S. at 56. Likewise, search must be confined in scope to find items relevant to the specific crime at hand. <i>Nero v. State</i> , 144 Md. App. 333, 345-46 (2002). | Application need only include: 1) identity of investigative officer and agency; and 2) statement “that the information likely to be obtained is relevant to an ongoing criminal investigation.” §10-4B-03(b). |
| Neutral/detached magistrate must consider whether facts underlying probable cause have grown stale. <i>Patterson v. State</i> , 401 Md. 76, 92 (2007). | |
| Must satisfy nexus requirement, sufficiently linking place to be searched with suspicion of criminal activity. For instance, “a suspect's home cannot be searched unless there are facts supporting a reasonable inference that contraband might be found there.” <i>Agurs v. State</i> , 415 Md. 62, 87 (2010). | |
| Must describe with particularity the place to be search or person to be seized. <i>United States v. Grubbs</i> , 547 U.S. 90, 91 (2006). | |
| Accordingly, “general rule is that a warrant to search a multi-unit building is void unless it specifies the unit to be searched.” <i>Peters v. State</i> , 224 Md. App. 306, 343 (2015). | |
| Scope and intensity of search must parallel the place to be searched and items to be seized. “[T]he same meticulous investigation which would be appropriate in a search for two small canceled checks could not be considered reasonable where agents are seeking a stolen automobile or an illegal still.” <i>Harris v. United States</i> , 331 U.S. 145, 153 (1947). | |

For further differences between the two instruments, *compare* Md. Code (2015 West), Courts & Judicial Proceedings Article, § 10-4B-01 through 04 (pen register order directed towards a telecommunication company to “authorize the installation and use of a pen register or a trap and trace device for a period not to exceed 60 days); *with* Md. Code (2015 West), Criminal Procedure Article, § 1-203 (search warrant “shall be directed to a duly constituted police officer... authorize the police officer... to search the suspected person, building, apartment, premises, place, or thing and to seize any property found subject to seizure under the criminal laws of the State.”).

To say the least, the pen register order issued by Judge Barry Williams in this case could not authorize a Fourth Amendment search or seizure. Judges are presumed to know the law and apply it accordingly, *Mobuary v. State*, 435 Md. 417, 440 (2013); so, this Court can only presume that Judge Williams observed an “[a]pplication” captioned “For an Order Authorizing The Installation And Use of a Device Known as a Pen Register/Trap & Trace” and judged it accordingly. Judge Williams scrutinized the State’s application with the statutory pen register factors in mind. Judge Williams did not scrutinize the application for its probable cause, particularity, nexus, scope and intensity, or any other concern attendant to search warrants. In fact, the BPD likely captioned its application to obtain the more-lenient standard of review. The State cannot go back now and ascribe to Judge Williams a judicial function he did not perform.

Moreover, the order the State did receive cannot render the Hailstorm search reasonable in any sense of the word. **The search here was the transmission of a multi-directional signal into a multitude of homes, and into the cellular telephones inside of those homes, to query the phone's location information.** (T3 48-49, 52, 54). The BPD's application failed entirely to mention that fact. Judge Williams' order could not render reasonable a Fourth Amendment search that Judge Williams knew nothing about.

Ultimately, the BPD's disingenuous efforts cannot be rewarded in this case. Per its agreement with the FBI, the BPD was forbidden from providing Judge Williams with any information about Hailstorm, how it worked, or what officers intended to do with it. (Apx. 2). The pen register application was therefore nothing more than an attempt to "hide the ball." The BPD sought permission to use surreptitious, dragnet-style, surveillance technology to peer within the confines of countless homes and cell phones, the overwhelming majority of which had nothing to do with this case; but, it attempted to do so without mentioning the scope, intensity, or nature of the search. Nothing in the application even hints at the fact that the BPD could link directly to a phone within a home.

The pen register application was nothing more than that—an application for an order directing the installation of a pen register on telephone company property. The moment the BPD conducted surveillance with something other than a pen register, it exceeded the purview of the pen register order. The State cannot now transform that order into a quasi-search warrant; doing as much renders

meaningless the guarantee that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const., amend IV.

III. THE SUPPRESSION COURT CORRECTLY RULED THAT THE FRUIT OF THE HAILSTORM SEARCH WAS INADMISSIBLE AT MR. ANDREWS’ TRIAL.

Law enforcement’s use of a Hailstorm device to capture and locate a target cell phone constitutes a search under the Fourth Amendment. Police officers must obtain a search warrant authorizing the device’s use, not an artfully-crafted pen register order. The United States Department of Justice has recognized as much, requiring all federal authorities to obtain a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure before using a cell site simulation device. U.S. Dep’t of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, <http://www.justice.gov/opa/file/767321/download> (last accessed Dec. 30, 2015).

In the final handful of pages in its brief, the State works to soften the blow of this conclusion. It points out that the BPD obtained a search warrant for 5032 Clifton Avenue after discovering Mr. Andrews and arresting him there. As a result, the firearm discovered and seized pursuant to that search warrant is safe from suppression. According to the State, the warrant was valid, officers relied on

it in good faith, and Mr. Andrews' does not possess the standing to challenge it. The State's arguments are misguided.¹¹

A. There is no issue with standing.

On appeal, the State argues that it raised a challenge to Mr. Andrews' standing that was left unanswered. The State fails to mention, though, the questionable circumstances of how it raised its challenge; and, fails to mention that the prosecutor at the hearing did not dispute defense counsel's proffer that Mr. Andrews was an "overnight guest," essentially waiving any argument on appeal.

Recall that the State failed to respond in any meaningful way to defense counsel's 56-page motion to suppress. (T4 6). Defense counsel thus walked into the suppression hearing entirely unaware that the State would, or could, challenge Mr. Andrews' standing to attack the 5032 Clifton Avenue search warrant. After all, it was the State's theory that Mr. Andrews possessed some property interest in 5032 Clifton Avenue. Moreover, statements provided by the State in discovery, upon which the State was relying for its case, made clear that Mr. Andrews was an overnight guest. (T4 42-43). An overnight guest possesses standing to challenge the search of his accommodations. *Minnesota v. Carter*, 525 U.S. 83, 90 (1998).

The State continued its silence on the issue of standing at the outset of the suppression hearing. It informed the suppression court that "there is nothing

¹¹ The State's arguments on pages 24-31 of its brief relate only to suppression of the gun. By their own terms, the arguments bear nothing on the challenge to the initial search—the use of the Hailstorm device—and the direct fruit of that search.

new”—no new testimony needed to be taken that day because the Fourth Amendment challenge could be decided on transcripts of the testimony given at the earlier discovery hearings. (T4 12-13). Defense counsel stipulated that the issue could be decided on the transcripts, so Judge Ausby accepted into the record the three discovery hearing transcripts. (T4 16). Thereafter, the State submitted into the record the arrest warrant issued for Mr. Andrews, “the actual DNR application” that was referenced in Detective Haley’s prior testimony, and the search warrant for 5032 Clifton Ave. (T4 24-26). With that, the fact-finding portion of the hearing concluded.

Only then did the State launch its salvo, asserting for the first time that Mr. Andrews lacked standing to challenge the search of 5032 Clifton Avenue. (T4 27). Judge Ausby did not “refuse to entertain the standing challenge.” (Appellant’s Brief at 24). She asked defense counsel to address the issue of Mr. Andrews’ standing. (T4 42). Defense counsel complied, responding that it had been the State’s theory all along that Mr. Andrews maintained a possessory interest in 5032 Clifton, that the State provided statements in discovery supporting that theory, and that she was caught off-guard because: “the State didn’t respond with a substance of a pleading. The State’s now asserting standing for the first time.” (T4 42-44).

Finally, defense counsel proffered that Mr. Andrews was an overnight guest at 5032 Clifton Avenue. (T4 44). In addition, defense counsel offered: if the suppression court wanted to “reopen” the record to take testimony, she would put Mr. Andrews on the stand to testify that he was an overnight guest. *Id.* The

suppression court impliedly declined to take more testimony, breaking for a recess before ultimately ruling on the motion.

At no point did the State challenge defense counsel's proffer. It conceded that the State's theory was "that he has some interest there and that is why the gun from this crime, the murder weapon, was there with him." (T4 43). It nonetheless claimed that such a theory was "for trial," and that defense counsel had to nonetheless prove standing by a preponderance. *Id.*

The State made an empty challenge in the suppression court. It possessed no serious, credible basis for challenging Mr. Andrews' standing there. It possesses no serious, credible basis now for asserting "[t]his was not Andrews's home." (Appellant's Brief at 24). The State failed to raise its argument in a timely manner and it failed to refute, in any way, defense counsel's proffer to the contrary. There can be no serious doubt that Mr. Andrews was an overnight guest at 5032 Clifton Avenue and the State has waived any argument otherwise. *See Joyner v. State*, 208 Md. App. 500, 512 (2012) ("[W]aiver is the intentional relinquishment or abandonment of a known right.").

Moreover, the State specifies no remedy for the error it alleges. That is because limited remand is the only reasonable outcome of this issue being decided in the State's favor. If the problem here is the suppression court's oversight in not hearing Mr. Andrews testify, "I was an overnight guest," the solution is remand to the suppression court for the taking of that testimony. After all, this is a factual matter defense counsel offered expressly to prove in the suppression court, but

could not do so through no fault of her own. Such a situation, especially in the context of first-level fact-finding that underlies a Fourth Amendment ruling, are ripe for limited remand. Md. Rule 8-604(d); *see also Collins v. State*, 138 Md. App. 300, 312-13 (2001) (limited remand for suppression court to make finding on consent to enter home); *Thompson v. State*, 139 Md. App. 501, 523-24 (2001) (limited remand for suppression court to make finding on whether warrant was validly signed).

B. The subsequent search warrant was fruit of the poisonous tree.

The State forwards a tortured argument, asserting that the search warrant for 5032 Clifton Avenue remained valid because police legally arrested Mr. Andrews pursuant to an arrest warrant. This misses the point. This Fourth Amendment challenge targets the use of a Hailstorm device and seeks to suppress the fruit of that search: the location data obtained from Mr. Andrews' cell phone. Without that location data, the BPD possessed no nexus between the criminal activity at hand and 5032 Clifton Avenue. Because the search warrant relied entirely on that nexus, it withers as fruit of the poisonous tree. Judge Ausby's ruling was absolutely correct.

Both this Court and the Court of Appeals have confronted, numerous times, the constitutional viability of a search warrant based on information obtained in an unconstitutional manner. *See e.g. Williams v. State*, 372 Md. 386, 409- 415 (2002); *see also e.g. Redmond v. State*, 213 Md. App. 163, 190-94 (2013). Even the

Supreme Court has faced such a case. *Karo*, 468 U.S. at 719. Each time, the analysis was nothing more than decision regarding whether the search warrant qualified as fruit of the poisonous tree—whether the illegally obtained evidence or knowledge was used “to establish probable cause for the issuance of [the] subsequent warrant. *State v. Klingenstein*, 92 Md. App. 325, 360 (1992) *aff’d in part, reversed in part on other grounds* 330 Md. 402 (1993). The State may only prevail, in cases like this, if the warrant issued on some source independent from the constitutionally tainted knowledge. *Williams*, 372 Md. At 410.

The fruit-of-the-poisonous tree analysis proceeds by looking to see “whether after the constitutionally tainted information is excised from the warrant, the remaining information is sufficient to support a finding of probable cause.” *Redmond*, 213 Md. App. at 191-92 (emphasis added). If the remainder cannot support a finding of probable cause, the warrant is declared invalid and its fruits are suppressed. *Id.* At 192-93. Only where the remainder qualifies as “sufficient untainted evidence...to establish probable cause” will the warrant and its fruits escape suppression. *Karo*, 468 U.S. at 719.

Applied to this case, the analysis is simple. Use of the Hailstorm imparted to the BPD knowledge of Mr. Andrews’ presence at 5032 Clifton Avenue. That knowledge must be excised from the search warrant. In the absence of that knowledge, there existed no probable cause to search 5032 Clifton Avenue. There existed, literally, no other reason to believe evidence of a crime would be found in that home. Mr. Andrews’ presence was the only connection between the home and

the crime under investigation. The knowledge derived from the illegal search formed the entire basis for the 5032 Clifton Avenue search warrant.

After excising Mr. Andrews' presence at 5032 Clifton from the search warrant, essentially excising the address from the search warrant, there is not sufficient information remaining to support a "fair probability that contraband or evidence of a crime [would] be found in [that] particular place." *Gates*, 462 U.S. at 238. Judge Ausby ruled correctly that the search warrant falls as fruit of the poisonous tree. The gun found and seized pursuant to that warrant must remain suppressed.

C. Good Faith is not applicable.

Though creative, the State's cursory good faith argument is inapplicable to this case. The *United State v. Leon* good faith exception is not applicable whenever a warrant is inadequate, as the State asserts. (Appellant's Brief at 29-30). "It is important to understand that *Leon* does not hold that the exclusionary rule is totally inapplicable whenever the search or seizure objected to was in some sense incident to a previously issued warrant." LaFave, *supra* at § 1.3(f).

Instances where good faith is not applicable include where a warrant falls as fruit of the poisonous tree. As this Court has explained: "in the case of an 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*." *Fitzgerald v. State*, 153 Md. App. 601, 656 (2003) *aff'd* by 384 Md. 484 (2004). Courts of other jurisdictions have nearly

unanimously held the same. *United States v. McGough*, 412 F.3d 1232, 1239-40 (11th Cir. 2005); *United States v. Scales*, 903 F.2d 765, 768 (10th Cir. 1990); *United States v. Vasey*, 834 F.2d 782, 788-89 (9th Cir. 1987); *State v. DeWitt*, 910 P.2d 9, 14-15 (Ariz. 1996); *State v. Carter*, 630 N.E.2d 355 (Ohio 1994); *State v. Johnson*, 716 P.2d 1288, 1298-1300 (Idaho 1986); *State v. Scull*, 639 So.2d 1239, 1245 (La. Ct. App. 1994).

Nor could good faith apply to a situation in which law enforcement officers, from the outset, dealt dishonestly with the judiciary. According to the State, the gun in this case was seized pursuant to a warrant based on knowledge obtained from a search authorized by a judicial filing. But step one—the judicial filing—was not made in good faith. The BPD withheld material facts from its pen register application with the express purpose of obtaining the judiciary’s leave to use a Hailstorm device. That type of behavior cannot result in “good faith” reliance on the neutral determination of a magistrate. This Court cannot endorse such a result.

CONCLUSION

For the foregoing reasons, Appellee requests that this Court affirm the ruling of the court below.

Respectfully submitted,

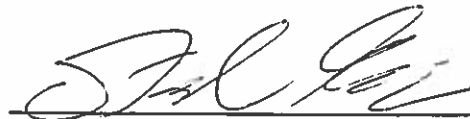
Paul B. DeWolfe
Public Defender

Daniel Kobrin
Assistant Public Defender

Counsel for Appellee

**CERTIFICATION OF WORD COUNT
AND COMPLIANCE WITH RULE 8-112**

1. Pursuant to Maryland Rule 8-503(d)(2), Appellee's Motion to Dismiss contains 629 words.
2. Pursuant to this Court's order, this brief contains 12,998 words, excluding the parts of the brief exempted from the word count by Rule 8-503.
3. This brief complies with the font, spacing, and type size requirements stated in Rule 8-112.



Daniel Kobrin

APPENDIX

UNCLASSIFIED//FOUO//LAW ENFORCEMENT SENSITIVE//NOFORN



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D C 20535-0001

July 13, 2011

Frederick H. Bealefeld, III
Police Commissioner
Baltimore Police Department
601 East Fayette Street
Baltimore, Maryland 21202-4014

Gregg L. Bernstein, Esq.
State's Attorney
Office of the State's Attorney for Baltimore City
110 North Calvert Street
Baltimore, Maryland 21202

Re: Purchase Wireless Collection Equipment/Technology and Non-Disclosure
Obligations

Dear Commissioner Bealefeld and Mr. Bernstein:

We have been advised by the Harris Corporation of the Baltimore Police Department's request to purchase certain wireless collection equipment/technology manufactured by Harris. Consistent with the conditions on the equipment authorization granted to Harris by the Federal Communications Commission (FCC), state and local law enforcement agencies must coordinate with the Federal Bureau of Investigation (FBI) to complete this non-disclosure agreement prior to the acquisition and use of the equipment/technology authorized by the FCC authorization.

As you are aware, law enforcement agencies increasingly rely on wireless collection equipment/technology to conduct lawfully-authorized electronic surveillance. Disclosing the existence of, and the capabilities provided by, such equipment/technology to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation wherein this equipment/technology is used to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other individuals, but also adversely impact criminal and national security investigations. That is, disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations. In order to ensure that such 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 by not limited to: in press releases, in court

UNCLASSIFIED//FOUO//LAW ENFORCEMENT SENSITIVE//NOFORN

UNCLASSIFIED//FOUO//LAW ENFORCEMENT SENSITIVE//NOFORN

documents, during judicial hearings, or during other public forums or proceedings. Accordingly, the Baltimore Police Department agrees to the following conditions in connection with its purchase and use of the Harris Corporation equipment/technology:

1. The Baltimore Police Department will ensure that operators of the equipment have met the operator training standards identified by the FBI and are certified to conduct operations.
2. The Baltimore Police Department will coordinate with the FBI in advance of its use of the wireless collection equipment/technology to ensure de-confliction of respective missions.
3. The Baltimore Police Department will not distribute, disseminate, or otherwise disclose any information concerning the wireless collection equipment/technology or any software, operating manuals, or related technical documentation (including its technical/engineering description(s) and capabilities) to the public, including to any non-law enforcement individuals or agencies.
4. The Baltimore Police Department will not distribute, disseminate, or otherwise disclose any information concerning the wireless collection equipment/technology or any software, operating manuals, or related technical documentation (including its technical/engineering description(s) and capabilities) provided to it to any other law enforcement or government agency without the prior written approval of the FBI. If approved, prior to any distribution, dissemination, or comparable disclosure of any information concerning the wireless collection equipment/technology or any software, manuals, or related technical documentation related to such equipment/technology, all materials shall be marked "Law Enforcement Sensitive, For Official Use Only - Not to be Disclosed Outside of the Baltimore Police Department."
5. The Baltimore Police Department and Office of the State's Attorney for Baltimore City shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of 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. If the Baltimore Police Department or the Office of the State's Attorney for Baltimore City learns that a District Attorney, prosecutor, or a court is considering or intends to use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology in a manner that will cause law enforcement sensitive information relating to the technology to be made known to the public, the Baltimore Police Department and/or Office of the State's Attorney for Baltimore City will immediately notify the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise.

Notification shall be directed to the attention of:

Assistant Director
Operational Technology Division
Federal Bureau of Investigation

UNCLASSIFIED//FOUO//LAW ENFORCEMENT SENSITIVE//NOFORN

UNCLASSIFIED//FOUO//LAW ENFORCEMENT SENSITIVE//NOFORN

Engineering Research Facility
Building 27958A, Pod A
Quantico, Virginia 22135
(703) 985-6100

and

Unit Chief
Tracking Technology Unit
Operational Technology Division
Federal Bureau of Investigation
Engineering Research Facility
Building 27958A, Pod B
Quantico, Virginia 22135
(703) 985-2602

In addition, the Baltimore Police Department, in conjunction with the Office of the State's Attorney for Baltimore City will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to use or provide, any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (beyond the evidentiary results obtained through the use of the equipment/technology), if using or providing such information would potentially or actually compromise the equipment/technology.

6. A copy of any court order in any proceeding in which the Baltimore Police Department or Office of the State's Attorney for Baltimore City is a party directing disclosure of information concerning the Harris Corporation equipment/technology and any associated software, operating manuals, or related documentation (including its technical/engineering description(s) and capabilities) will immediately be provided to the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise. Any such court orders shall be directed to the attention of:

Assistant Director
Operational Technology Division
Federal Bureau of Investigation
Engineering Research Facility
Building 27958A, Pod A
Quantico, Virginia 22135
(703) 985-6100

and

Unit Chief
Tracking Technology Unit
Operational Technology Division
Federal Bureau of Investigation
Engineering Research Facility
Building 27958A, Pod B
Quantico, Virginia 22135
(703) 985-2602

UNCLASSIFIED//FOUO//LAW ENFORCEMENT SENSITIVE//NOFORN

UNCLASSIFIED//FOUO//LAW ENFORCEMENT SENSITIVE//NOFORN

7. The Baltimore Police Department will not publicize its purchase or use of the Harris Corporation equipment/technology or any of the capabilities afforded by such equipment/technology to the public, other law enforcement agencies, or other government agencies, including, but not limited to, in any news or press releases, interviews, or direct or indirect statements to the media.
8. In the event that either the Baltimore Police Department or the Office of the State's Attorney for Baltimore City receives a request pursuant to the Freedom of Information Act (5 U.S.C. § 552) or an equivalent state or local law, the civil or criminal discovery process, or other judicial, legislative, or administrative process, to disclose information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities), the Baltimore Police Department will immediately notify the FBI of any such request telephonically and in writing in order to allow sufficient time for the FBI to seek to prevent disclosure through appropriate channels. Notification shall be directed to the attention of:

Assistant Director
Operational Technology Division
Federal Bureau of Investigation
Engineering Research Facility
Building 27958A, Pod A
Quantico, Virginia 22135
(703) 985-6100

and

Unit Chief
Tracking Technology Unit
Operational Technology Division
Federal Bureau of Investigation
Engineering Research Facility
Building 27958A, Pod B
Quantico, Virginia 22135
(703) 985-2602

The Baltimore Police Department's, and the Office of the State's Attorney for Baltimore City's acceptance of the above conditions shall be evidenced by the signature below of an authorized representative of the respective agencies.


Sincerely,

Ernest Reith
Acting Assistant Director
Operational Technology Division
Federal Bureau of Investigation

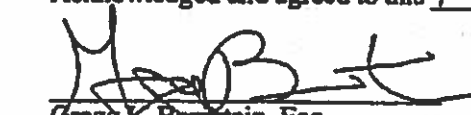
UNCLASSIFIED//FOUO//LAW ENFORCEMENT SENSITIVE//NOFORN

UNCLASSIFIED//FOUO//LAW ENFORCEMENT SENSITIVE//NOFORN

Acknowledged and agreed to this 11th day of August, 2011,


Frederick H. Bealefeld, III
Police Commissioner
Baltimore Police Department

Acknowledged and agreed to this 10th day of August, 2011,


Gregg K. Bernstein, Esq.
State's Attorney
Office of the State's Attorney for Baltimore City

cc: Barry F. Kroboth, Unit Chief, FBI Tracking Technology Unit
Valerie M. Barrish, FBI Office of the General Counsel
Joseph W. Mazel, FBI Office of the General Counsel
Sheryl Goldstein, Director, City of Baltimore Mayor's Office on Criminal Justice

UNCLASSIFIED//FOUO//LAW ENFORCEMENT SENSITIVE//NOFORN

CITY OF BALTIMORE

STEPHANIE RAWLINGS-BLAKE, Mayor



DEPARTMENT OF LAW

GEORGE A. NILSON, City Solicitor
101 City Hall
Baltimore, Maryland 21202

October 21, 2015

Ms. Natalie Finegar
Office of the Public Defender
201 St. Paul Place - 5th Floor
Baltimore, MD 21202

Re: Maryland Public Information Request

Dear Ms. Finegar,

In your September 15, 2015 letter addressed to the Baltimore Police Department ("BPD"), Custodian of Records, Legal Affairs, received by the Office of Legal Affairs on September 21, 2015, you made eleven (11) separate requests for records pertaining to the Baltimore Police Departments use of cell site simulator technology. The Maryland Public Information Act ("MPIA"), Annotated Code of Maryland, General Provisions Article, § 4-101, et seq. governs your request.

Each one of your separate requests is addressed below as follows:

Request Number 1: Records regarding the Baltimore Police Department's ("BPD") acquisition of cell site simulators including invoices, purchase orders, contracts, loan agreements, solicitation letters, correspondence with companies providing the devices (both paper and electronic), and all similar documents or emails. In furtherance of this request, please produce records, of all contracts, agreements and communications with Harris Corporation, Digital Receiver Technology ("DRT") and any other company or subsidiary that has sold or contracted to sell cell site simulators to the BPD

BPD's Response to request Number 1: To the extent that your request seeks general records regarding BPD's "acquisition" of cell site simulator technology, the BPD will direct you to the following web links below, which detail BPD's purchase of the technology, through and approved by the Baltimore City Board of Estimates:

- *<http://comptroller.baltimorecity.gov/minutes/2009-02-04.pdf>
- *http://comptroller.baltimorecity.gov/minutes/1767-1899_2010-06-09.pdf
- *http://comptroller.baltimorecity.gov/minutes/0179-0279_2013-01-23.pdf

Additionally, the BPD Custodians have advised that they are not in possession of any responsive records regarding: "contracts", "loan agreements", "solicitation letters" regarding the acquisition of the cell site simulator technology.

The Custodian of Records for the Fiscal Section of BPD is still searching for responsive records pertaining to: "invoices" and "purchase orders" regarding the acquisition of the technology. If and when

same are located by that Unit, they will be reviewed and then forwarded under this request. If responsive records have not been located within thirty (30) days from the date of this response, this office will forward correspondence to requester that same could not be located.

As well, to the extent that your request seeks email communications, BPD will advise of the following:

Requests for BPD emails are handled by the Information and Technology Section ("IT"). BPD emails have a limited retrieval time frame. The I T technicians can retrieve emails for approximately the past two (2) calendar years going back from the date of the request. To retrieve emails outside of the past two calendar years, a private vendor must be retained to retrieve archived emails at a substantial cost.

The cost of in-house retrieval of emails is based on the number of emails that must be reviewed before being disclosed. Confidential opinions, deliberations, advice or recommendations from one governmental employee or official to another for the purpose of assisting the latter official in the decision-making function may be withheld. Communications that are part of and/or pertain to a police investigation may be withheld. In addition, part of an interagency, or intra-agency letter or memorandum that would not be available by law to a private party in litigation can be withheld.

The BPD can run a word, name or phrase through the email retention system. The BPD can run the search to include only individual email addresses or the entire BPD email system. Once the system identifies the emails with the word, name or phrase each email will have to be review to determine what can be disclosed and their relevancy.

To assist BPD in locating documents responsive to your request, it is necessary for you to provide BPD with search criteria in the form of key words/phrases to perform a search for potentially responsive records. It is in your interest to be as specific as possible when supplying key words/phrases to be ran through the search system, so as to filter out unresponsive communications from the total pool of communications returned by the search.

MPIA Section 4-206 permits the BPD to charge reasonable fees for the time associated with searching and preparing responsive documents for your request. The BPD charges \$50/hour for the time required to search for and prepare the responsive records, excluding the first two (2) hours searching for and preparing the responsive records. The normal amount of time required to review Thirty (30) pieces of correspondence is around one (1) hour of staff time. After responsive records are retrieved from the initial search, BPD will use the above time quote to provide you with the appropriate cost estimate to complete the request. There is a minimum charge of \$50.00 to start the search and downloading of emails. The \$50.00 will be applied to the final cost. If the costs and terms are agreed upon emails will be reviewed.

Request Number 2: Any and all training materials and operating manuals for any cell site simulator used by the BPS.

BPD's Response to Request Number 2: The Custodian has advised that to the extent that your request seeks documents pertaining to "training materials", BPD is not in possession of any responsive documents.

To the extent that your request seeks production of "Operating Manuals" for the cell site simulator technology, the BPD must deny your request pursuant to MPIA § 4-335, as the release of confidential proprietary information is prohibited by a Governmental entity. Additionally, the release of any technical information concerning the capability of the technology may violate the *Arms Control Export Act and International Traffic In Arms Regulation (ITAR)*. Pursuant to ITAR, the manufacturers of cell site simulator technology have classified these devices as regulated defense articles on the United States Munitions List ("USML"). See 22 C.F.R. § 121.1(b). As such, technical details concerning this technology are subject to the non-disclosure provisions of the ITAR, 22 C.F.R., Parts 120-130.

Request Number 3: Records regarding any offer, arrangement or agreement with the Federal Bureau of Investigation ("FBI") or any corporation to borrow or use cell site simulators owned or possessed by the FBI or corporation.

BPD's Response to Request Number 3: The BPD is not in possession of any records responsive to this request.

Request Number 4: All memoranda of understanding, nondisclosure agreements, contracts, or other agreements with the FBI or any other state, local or federal agency regarding the BPD's possession and use of cell site simulators

BPD's Response to Request Number 4: Enclosed are the records the Custodian has determined as responsive to this request; July 13, 2011 Non-Disclosure Agreement executed between the FBI and then Commissioner Bealefeld and then State's Attorney Greg Bernstein.

Request Number 5: All nondisclosure agreements with Harris Corporation, DRT or any other companies regarding the BPD's possession and use of cell site simulators.

BPD's Response to Request Number 5: The BPD is not in possession of any records responsive to this request.

Request Number 6: Records regarding policies and guidelines governing the use of cell site simulators, including (but not limited to) restrictions on when, where, how, and against whom they may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of cell site simulators may be revealed to the public, criminal defendants or judges. If these policies and guidelines have changed, please provide each and every version of every policy and guideline generated and the dates in which said policy and/or guideline was in effect.

BPD's Response to Request Number 6: The BPD is not in possession of any records responsive to this request. The BPD will note that the General Assembly added to Maryland Code, Criminal Procedure Article, §1-203.1 "Location information obtained from electronic devices" effective October 1, 2014, which governs the application for and issuance of court order's authorizing a law enforcement agency such as BPD to obtain location information from an electronic device.

Request Number 7: Records regarding any communications, licenses, waivers or agreements with the Federal Communications Commission regarding the use of cell site simulators.

BPD'S Response to Request Number 7: The BPD is not in possession of any records responsive to this request.

Request Number 8: Records reflecting the number of investigations in which cell site simulators have been used, and the number of those investigations that have resulted in prosecutions.

BPD'S Response to Request Number 8: Enclosed are records responsive in part to your request, which reflect the BPD's Advanced Technical Team's ("ATT") "log" of investigations that unit maintains to monitor requests by other investigative units of BPD, i.e. Patrol Division, District Detective Units, Homicide, etc., for cell phone related assistance. Each individual entry in the report does not represent that the technology was employed in every entry/investigation. As the record reflects, entries that note "captured", are investigations where the technology was employed. To the extent that the record contained personal cell phone numbers of victims/witnesses, those have been removed and are being withheld pursuant to MPLA Section 4-351(b).

The BPD is not in possession of one identifiable record that could be provided under this request as responsive to your request for "the number of those investigations that have resulted in prosecutions". As the record reflects "CC_Num" column, such information may be used to obtain other police records/Court Records which may aid you in locating responsive records to this portion of your request.

Request Number 9: Records reflecting a list of all criminal cases, with case numbers if available, in which law enforcement officers used a cell site simulator as part of the underlying investigation.

BPD's Response to Request Number 9: Please see BPD's response to Request number 8, adopted as BPD's response to this request.

Request Number 10: All applications submitted to state or federal courts for search warrants or orders authorizing use of cell site simulators in criminal investigations, as well as any warrants or orders, denials of warrants or orders and returns of warrants associated with those applications. If any responsive records are sealed, please provide the date, jurisdiction and docket number for each sealed document.


BPD's Response to Request Number 10: The Custodian of the records responsive to your request is the Clerk of the Court. The Clerk of the Court maintains the Applications and Orders. To this end, you may use the records provided herein to search for responsive Court Records to this request.

Request Number 11: All records regarding the use of cell site simulators in closed investigations

BPD's Response to Request Number 11: Please see BPD's response to request numbers 8 and 9, adopted as its response to request number 11.

Nothing in this response is intended to indicate that any records sought from the BPD exist or to waive any privileges held by the BPD. You may contest this response by filing a complaint for Judicial Review in Circuit Court pursuant to MPLA Section 4-362.

Sincerely,


Brent Schubert

**Assistant City Solicitor
Legal Affairs Division
Baltimore Police Department
100 N. Holliday Street, Room 101
Baltimore, Maryland 21202**

