State of Maryland v. Robert L. Copes, Jr.
No. 84, September Term 2016

Search and Seizure – Warrant Requirement – Exclusionary Rule – Good Faith Exception. Police officers applied for court authorization to use a cell site simulator and other techniques to locate a missing cell phone associated with a murder victim in the hope that the phone would lead them to the murderer. They obtained a court order, based in part on the procedure required for obtaining court authorization for a pen register under the Maryland Pen Register Statute, Maryland Code, Courts & Judicial Proceedings Article, §10-4B-01 *et seq.* Using the cell site simulator, the police succeeded in locating the cell phone, together with Respondent Robert L. Copes, Jr., and evidence linking him to the victim and the murder. The Circuit Court later concluded that the use of the cell site simulator violated the Fourth Amendment and suppressed the evidence. The Court of Appeals assumed, for the sake of argument, that use of a cell site simulator by law enforcement officers is a search for purposes of the Fourth Amendment. The Court concluded that, even if the court order under the Pen Register Statute fell short of a search warrant, the officers engaged in "objectively reasonable law enforcement activity" in obtaining the order and using the cell site simulator to locate the cell phone. Under the good faith exception to the exclusionary rule, the evidence would not be suppressed.

Circuit Court for Baltimore City
Case 114090005
Argument: April 3, 2017

IN THE COURT OF APPEALS
OF MARYLAND

No. 84

September Term, 2016

STATE OF MARYLAND

v.

ROBERT L. COPES, JR.

Barbera, C.J.
Greene
Adkins
McDonald
Watts
Hotten
Getty,

JJ.

Opinion by McDonald, J.
Greene, Adkins, and Hotten, JJ., dissent.

Filed: July 28, 2017

Advances in personal technology, like the cell phone, empower individual users but may also threaten personal privacy. When police make use of the features of that technology to solve crime, courts and lawyers sometimes struggle to devise ground rules that respect constitutional privacy protections. This case involves an example of the law's effort to keep apace.

Detectives investigating the gruesome murder of a young homeless woman in Baltimore City determined that a cell phone associated with her – but not found with her body – was still in active use. Hoping to find the phone – and the murderer – they applied to the Circuit Court for authorization to use, among other techniques, a "cellular tracking device" to locate the phone. They presented a sworn application to the Circuit Court that summarized the investigation of the murder, information concerning the missing phone, and their purpose in attempting to find it, as well as a draft order that tracked the application in pertinent respects. They did so under an established procedure – approved by the State's Attorney and the Police Department's lawyer – that had been adapted from a statute for police use of devices that record the numbers of incoming and outgoing calls concerning a target phone. The court issued the order, finding that "probable cause exists" upon the basis of the application.

The detectives then employed a device known as a cell site simulator – basically, an undercover cell tower – which led them to the apartment of Respondent Robert L. Copes, where they found the phone, Mr. Copes, and evidence linking him to the victim and the murder.

After charges were filed, Mr. Copes asked the Circuit Court to suppress the evidence obtained as a result of the use of the cell site simulator. Despite finding that the detectives acted "in good faith" and had done "fine work," the Circuit Court felt constrained by a recent decision of the Court of Special Appeals.[1] It granted the motion on the ground that the use of the cell site simulator to locate the phone was a search for purposes of the Fourth Amendment and that the court order did not function as a search warrant.

We hold that the evidence need not be suppressed. Regardless of whether use of a cell site simulator is a search for purposes of the Fourth Amendment or whether the court order authorizing its use fell short of a search warrant, the detectives in this case acted in "objectively reasonable good faith."

I

Background

A. Cell Site Simulators and Judicial Authorization for Location Tracking

1. Cell Phones and Location Tracking

The ubiquitous cell phone has become a necessity of modern life. It facilitates mobility and access to information, not to mention mobile access to information. It has also spawned much attention in the application of the constitutional protections of personal privacy. Much of that attention concerns the information contained on a cell phone,

[1] *State v. Andrews*, 227 Md. App. 350 (2016).

particularly a "smart phone" that may contain or access a library of private information.[2] Of equal concern is the ability of the cell phone to transmit information about its location – and the location of the individual who possesses it.

A cell phone's identification of its location is one of its essential virtues. A cell phone must be found by a service provider for it to be used as a phone. The location tracking feature of a cell phone is commonly used by those with a cell phone to navigate,[3] to locate an errant cell phone,[4] to find friends or family with cell phones in the vicinity,[5] and to summon help to the location of the cell phone in an emergency.[6]

---

[2] *See Riley v. California*, ___ U.S. ___, 134 S.Ct. 2473 2489-91 (2014); *Sinclair v. State*, 444 Md. 16 (2015).

[3] Without the location tracking function, a cell phone could not offer real-time navigation. Aggregation of such data from many cell phones allows various navigation applications to provide traffic updates.

[4] *See, e.g.,* James Bruce, *"How to Use Find My iPhone to Get Your Stolen iPhone Back"* (November 6, 2011). http://www.makeuseof.com/tag/find-iphone-stolen-iphone/ [https://perma.cc/8E3N-S7SH].

[5] A number of cell phone applications use the location tracking features of cell phones to inform a cell phone user when friends or acquaintances with cell phones happen to be in his or her geographic vicinity. For example, such a feature is built into the maps function in Snapchat. *See* Kurt Wagner, *"How to Use – and How to Keep Yourself Hidden from – Snapchat's New Maps Feature,"* (July 6, 2017). https://www.recode.net/017/7/6/15929952/how-to-use-hide-ghost-mode-snapchat-snap-maps-location-privacy. [https://perma.cc/5PFR-85NU].

[6] The Federal Communications Commission is requiring wireless service providers to provide precise location information of cell phones to public safety agencies in connection with 911 calls. *See* https://www.fcc.gov/consumers/guides/911-wireless-services [https://perma.cc/FZ3J-WMAV].

Law enforcement has sought to enlist this feature of cell phones to prevent and investigate crime. This case involved the use of two techniques that depend on a cell phone's indication of its location: cell site location information obtained from a service provider and a device known generically as a cell site simulator.

Cell Site Location Information ("CSLI")

When a cell phone sends or receives a call or text message, it attempts to connect with the service provider's closest cell tower.[7] If one knows which cell towers a cell phone has connected to (or is connecting to) and the physical location of those towers, one can approximate the geographical location of that cell phone. This information is often referred to as "cell site location information" or "CSLI." Information concerning which towers a cell phone has connected to in the past is sometimes referred to as "historical CSLI." Information concerning which towers a cell phone is currently connecting to is sometimes referred to as "real-time CSLI."[8]

Cell Site Simulators

A cell site simulator works as its name suggests – it pretends to be a cell tower on the network of the target phone's service provider.[9] It takes advantage of the fact that a

---

[7] *See State v. Payne*, 440 Md. 680, 691-97 (2014).

[8] A service provider may collect CSLI passively as part of its normal business operations. A provider may also actively monitor the location of a phone on its network by "pinging" a phone. *See* S. K. Pell & C. Soghoian, *Can You See Me Now?: Towards Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 Berkeley Tech. L. J. 117, 131-32 (2012).

[9] The various versions of cell site simulators have apparently been given names by their manufacturers – such as "Stingray" and "Triggerfish." The model of cell site

cell phone – when turned on –constantly seeks out nearby cell towers, even if the user is not making a call.[10] Furnished with identifying information concerning the target phone, the cell site simulator searches for that phone. When the cell site simulator is close enough, the target phone will connect to it as though it were a cell tower.[11]

Law enforcement officers using a cell site simulator may employ two devices in tandem: one stationed in a vehicle, the other carried by hand. The vehicular device, when it makes a connection with the target phone, points the user in the direction of the target phone. The handheld device, when taken in that direction, informs the user whether the target phone is getting closer or farther away. The combination of the two devices can produce a fairly accurate estimate of the target phone's location.[12]

---

simulator used in this case was called "Hailstorm" and was manufactured by the Harris Corporation. We understand that, for purposes of this opinion, any technological differences among these models are insignificant.

[10] *See* Staff of House Committee on Oversight and Government Reform, 114th Cong., Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations (2016) at 10 , https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf [https://perma.cc/AF7C-465V].

[11] Other cell phones in that range may or may not also attempt to connect with the cell site simulator. However, because the cell site simulator has been programmed to look only for the target phone, the cell site simulator declines to maintain a connection with those phones.

[12] It also may be possible to configure particular cell site simulators to intercept data or communications. *See generally* S. K. Pell & C. Soghoian, *A Lot More Than a Pen Register, and a Lot Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J.L. & Tech. 134, 146 (2013). According to testimony at the hearing in this case, the cell site simulator used in this case did not have that capability.

2. Orders Authorizing Location Tracking under the Pen Register Statute

At the time of the investigation in this case, no statute specifically addressed the use of a cell site simulator or other device to track a cell phone's location.[13] Apparently, many law enforcement agencies, including the Baltimore City Police Department and the United States Department of Justice,[14] obtained judicial authorization to use a cell site simulator by following the established procedures for obtaining authorization to use a pen register or trap and trace device. As we shall see, some modifications and enhancements were made to a standard pen register application and order to customize those documents to a cell site simulator. We take a short detour to describe the Maryland Pen Register Statute, Maryland Code, Courts & Judicial Proceedings Article ("CJ"), §10-4B-01 *et seq.*

In simple terms, a pen register records the numbers dialed out from a given phone, and a trap and trace device records the numbers that dial into that phone. *See* CJ §10-4B-01(c), (d) (definitions of "pen register" and "trap and trace device"). When information from both devices is aggregated, a log of all incoming and outgoing calls can be created for the period that the devices are active. These devices do not capture the content of

---

[13] A statute was later enacted. *See* Part I.A.3 of this opinion below.

[14] *See* U.S. Dep't of Justice, Electronic Surveillance Manual; Procedures; Case Law 46, https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-anual.pdf [https://perma.cc/SC85-EHL7]. In 2015, however, the Department changed that policy to require federal law enforcement officers to obtain a warrant before using a cell site simulator. U.S. Dep't of Justice, *Justice Department Announces Enhanced Policy for Use of Cell site Simulators* (Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell site-simulators [https://perma.cc/KX4S-HFP2].

communications. The Fourth Amendment does not require law enforcement officers to obtain a search warrant in order to use a pen register or trap and trace device. *Smith v. Maryland*, 442 U.S. 735 (1979).[15] Nevertheless, the General Assembly, by enacting the Pen Register Statute,[16] has required law enforcement officers to obtain judicial approval before using a pen register or a trap and trace device in an investigation.[17]

To obtain an order under the Pen Register Statute, a law enforcement officer must make application under oath to a "court of competent jurisdiction in the State." CJ §10-4B-03(a). The application must identify the officer and agency conducting the investigation, and must state that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. CJ §10-4B-03(b). Unlike an application for a search warrant, the application to use a pen register or trap and trace device need not demonstrate probable cause that a crime has been committed or that the

---

[15] In *Smith*, the Supreme Court held that a telephone user has no legitimate expectation of privacy in numbers dialed from the user's phone, because the user voluntarily shares those numbers with a third party – *i.e.*, the telephone company. The Court held that law enforcement use of a pen register to record those numbers is not a Fourth Amendment search and, correspondingly, does not require a warrant. That reasoning has come to be known as the "third party doctrine."

Although the Supreme Court has never decided whether the use of a trap and trace device is a Fourth Amendment search, lower courts applying the third party doctrine have held that use of trap and trace device is not a search and that a warrant is not required. *See, e.g.*, *United States v. Hallmark*, 911 F.2d 399, 402 (10th Cir. 1990); *United States v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009); *Sun Kin Chan v. State*, 78 Md. App. 287 (1989).

[16] This statute governs the use of trap and trace devices, as well as pen registers.

[17] There is a parallel federal statute. 18 U.S.C. §3121 *et seq*.

evidence relating to that crime will be acquired through use of the device. If the application is approved, the order must identify the individual, if known, whose phone number is being surveilled and the individual who is the subject of the criminal investigation. CJ §10-4B-04(b). The order may authorize use of the device for a maximum of 60 days. CJ §10-4B-04(c). The statute also requires a phone service provider to whom an order is presented to furnish the officer with "all information, facilities, and technical assistance necessary to accomplish the installation" of the device "unobtrusively and with a minimum of interference" to the phone's service. CJ §10-4B-05(a)-(b).

3. CP §1-203.1

In 2014, the General Assembly enacted a statute to provide a specific judicial procedure to authorize law enforcement use of location tracking through cell phones. Chapter 191, Laws of Maryland 2014, *codified at* Maryland Code, Criminal Procedure Article ("CP"), §1-203.1. That statute provides for the District Court or a circuit court to authorize law enforcement officers "to obtain location information from an electronic device" in defined circumstances if the officers present a sworn application with a showing of probable cause, as specified in the statute. The statute became effective October 1, 2014, a few months after the events in this case. Since that time, law enforcement efforts to obtain judicial authorization for use of a cell site simulator presumably have been made pursuant to CP §1-203.1, as opposed to the format based on the Pen Register Statute. No appellate court has yet construed this statute or opined on its constitutionality.

B. The Investigation of the Murder of Ina Jenkins

The following information was elicited in testimony at the pretrial motions hearing in this case. For purposes of deciding the issues before us, it appears to be largely undisputed.

1. The Homicide

On February 4, 2014, a burned body was found in the rear yard of 4013 Penhurst Avenue, a vacant home in northwest Baltimore. Police found a black backpack containing a plastic bottle with some gasoline in a crawl space of the house about 10 to 15 feet from the body. Detective Bryan Kershaw of the homicide unit of the Baltimore City Police Department was assigned as lead investigator.

2. The Investigation

Identification and Autopsy

Fingerprint evidence identified the body as that of Ina Jenkins, a 34-year old homeless woman. The State Medical Examiner performed an autopsy and determined that Ms. Jenkins' death was a homicide by blunt force trauma and that her body had been burned after she died. Based on evidence gathered from the crime scene and elsewhere, Detective Kershaw suspected that Ms. Jenkins had been murdered at a nearby location and that her body had been bound, carried on foot to the yard of the vacant home, and set on fire sometime on January 20 or 21, 2014 – approximately two weeks before her body was discovered.

Videos of Ms. Jenkins with an Unidentified Man

Detective Kershaw learned that Ms. Jenkins frequently spent her days at My Sister's Place, a resource center for women and children in need run by Catholic Charities in downtown Baltimore, and at the Enoch Pratt Free Library across the street. She often spent her nights at what was called a "code blue" shelter.[18] Detective Kershaw obtained records of recent expenditures Ms. Jenkins had made with her Independence Card – a debit card for food stamps and other cash benefits – and obtained surveillance videos from those merchants. Videos from two different merchants showed Ms. Jenkins and an unidentified man shopping a few days before her death. In both videos, the man was wearing, in Detective Kershaw's words, a "very distinct" blue and yellow coat. Detective Kershaw also obtained records of books Ms. Jenkins had recently borrowed from the library.

Canvassing the Neighborhood of the Murder

During the week beginning Monday, February 10, 2014, detectives canvassed the Penhurst Avenue neighborhood during the day and night to find potential witnesses to the murder. Still photos from the surveillance videos were given to officers on patrol in the area in the hope that an officer might encounter and recognize Ms. Jenkins' unidentified companion – or, perhaps, his "very distinct" coat.

---

[18] When the Baltimore City Health Commissioner declares a "code blue" alert during periods of extreme cold weather, various steps are taken to extend the hours and capacity of homeless shelters. *See* Baltimore City Health Department, *Code Blue Alert Information*, http://health.baltimorecity.gov/emergency-preparedness-response/code-blue [https://perma.cc/RK35-QLKP].

During these canvasses, Detective Kershaw knocked on various doors in the neighborhood, including the doors to apartments 1-E and 1-W on the first floor of 4014 Penhurst Avenue, an apartment building directly across the street from the vacant home with the yard where Ms. Jenkins' body was found. On February 12, 2014, Detective Kershaw met with the tenant in apartment 1-W. That tenant advised Detective Kershaw that, although the second floor apartment in the building was vacant, apartment 1-E was occupied. There was no response when Detective Kershaw knocked on the door to apartment 1-E that day.

Telephones used by Ms. Jenkins

Detective Kershaw also interviewed Ms. Jenkins' mother, who provided several telephone numbers associated with her daughter. In a letter, Ms. Jenkins had provided her mother with a phone number ending in -8138. More recently, on January 19, 2014, a day or two before the murder, Ms. Jenkins had called her mother from another phone number, ending in -4686, according to the caller ID log in her mother's telephone. Neither phone had been found with Ms. Jenkins' body. The detectives decided to try to locate the phones in the hope that they would advance the investigation.

Court Order under the Pen Register Statute

On February 11, 2014, one of the detectives applied to the Circuit Court for Baltimore City for court orders related to the -8138 and -4686 numbers.[19] We shall focus

[19] Ms. Jenkins' mother had also provided a third phone number to Detective Kershaw. Detective Kershaw determined that the phone associated with the third number was out of service and therefore did not seek an order with respect to it.

on the order pertaining to the -4686 number, as that is the particular order that led to the discovery and apprehension of Mr. Copes and that is at issue in this case.

The sworn application was submitted under the Pen Register Statute. The application asked the court to authorize the "installation and use of a device known as a Pen Register/Trap & Trace and Cellular Tracking Device to include cell site information." In "support of probable cause for the interception of real-time cell site information," the detective provided a brief summary of the discovery of Ms. Jenkins' body and the results of the autopsy, reported that certain cell phone numbers were associated with Ms. Jenkins but that the phones associated with those numbers were not found with her body, and concluded that the phones were taken by the "unknown suspect(s) and were likely being used "until service is terminated or the phone becomes non-functional." The detective further asserted in the application that "records will assist in possibly identifying and locating the unknown suspect(s)" and that "the information likely to be obtained concerning the aforesaid individual's location will be obtained by learning the numbers, locations, and subscribers of the telephone number(s) being dialed or pulsed from or to the aforesaid telephone and that such information is relevant to the ongoing criminal investigation being conducted by [the Police Department]."

The application asked for an order directing cell phone service providers to provide necessary technical information to the police and asked the court for authorization to, among other things, "employ surreptitious duplication of facilities, technical devices or equipment to accomplish the use of a … Cellular Tracking Device, unobtrusively and with a minimum of interference to the subscriber of the … telephone, and … initiate a signal to

determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonably available, Global Position system Tracing and Tracking, Mobile Locator tools, R.T.T. (Real Time Tracking Tool), …Precision Locations and any and all locations …"

The Circuit Court issued the order the same day. In the order, the court found "that probable cause exists and that the applicant has certified that the information likely to be obtained . . . is relevant to an ongoing criminal investigation." The order authorized the installation and use of a "Pen Register/Trap & Trace and Cellular Tracking Device to include cell site information" for 60 days within the jurisdiction of the court, and also authorized the Police Department to obtain information about the cell phones from the pertinent service provider. Most pertinent to this case, the order authorized the detectives to "employ … [a] Cellular Tracking Device [and] initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonably available, Global Position System Tracing and Tracking, Mobile Locator tools, R.T.T. (Real Time Tracking Tool)…." with the same conditions and qualifications as requested in the application. In addition, the service provider was directed to "initiate a signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent/agencies serving this order."

Calling the Cell Phone

The detectives determined from the service provider – in this case Verizon – that the -4686 phone was a prepaid phone without an annual contract and that therefore there was no subscriber information available for that phone. Detective Kershaw called the -4686 number daily, without success until February 18, 2014, when a male voice answered the phone. Detective Kershaw hung up without speaking to the individual and immediately contacted Detective John Haley of the Police Department's Advanced Technical Team.

Obtaining CSLI for the Cell Phone

Pursuant to the court order, Detective Haley obtained from Verizon a list of calls and text messages sent or received by the -4686 phone. That list, which began with records starting around 7:30 p.m. that day, was created by Verizon and was updated in real time. In addition to noting the calls and text messages, the list also included CSLI – information concerning which cell towers the phone was connected to for each call and text message, as well as which area or "sector" of each tower's coverage the cell phone was using.

The list of calls and text messages made by the -4686 phone indicated that the phone was using two cell towers in Baltimore, one located at 2500 West Belvedere Avenue and the other at 4110 Menlo Drive. Combining that information with information about which sector of each tower's coverage the phone was using, Detective Haley and the Advanced Technical Team were able to trace the -4686 phone to the Penhurst Avenue neighborhood, where Ms. Jenkins' body had been found.

Using the Cell Site Simulator

After analyzing the CSLI and determining that the -4686 phone was in the Penhurst Avenue neighborhood, Detective Haley and the team, under directions from Detective Kershaw, drove a cell site simulator to that area. The cell site simulator consisted of two devices, one stationed in the Advanced Technical Team's police vehicle and a handheld device. The detectives punched into the cell site simulator the -4686 phone's identifying numbers, which they had obtained from Verizon pursuant to the court order. Detective Haley and the team then used the devices to narrow down the cell phone's location.

Using the vehicular device, Detective Haley and the Advanced Technical Team were able to make signal contact with the -4686 phone. The team then contacted Detective Kershaw, who came to the scene.[20] After his arrival, the detectives again used the cell site simulator – both the vehicular and the handheld devices – to track the -4686 cell phone. The devices indicated that the phone was at 4014 Penhurst Avenue – the apartment building across the street from the yard where Ms. Jenkins' body had been found and where Detective Kershaw had already questioned the residents other than the occupant of apartment 1-E.[21]

---

[20] When Detective Kershaw first arrived at 4014 Penhurst Avenue, he saw an individual, later identified as Perry Renwick, emerging from the back of that building. Detective Kershaw identified himself as a police officer, but Mr. Renwick fled back up the stairs. Detective Kershaw pursued him to a third floor apartment that was previously unknown to the detectives. Detective Kershaw spoke briefly with Mr. Renwick and noted that he was not the individual in the surveillance videos with Ms. Jenkins.

[21] The record is unclear as to whether the device allowed police to track the phone to a specific apartment or just to 4014 Penhurst Avenue generally. In any event, by the time Detective Kershaw arrived at the door to apartment 1-E that night, he had already met

Meeting Mr. Copes

At approximately 11:30 pm, Detective Kershaw knocked on the door to apartment 1-E, as he had earlier in the week. This time, the door was answered by Mr. Copes, clad in a t-shirt and boxer shorts. Detective Kershaw immediately recognized Mr. Copes as the man who had been accompanying Ms. Jenkins in the surveillance videos. He showed Mr. Copes a photo of Ms. Jenkins and explained that the Police Department was investigating her death. Mr. Copes said that he knew Ms. Jenkins from the "code blue" shelter.

Mr. Copes indicated that he wished to get dressed and the two men went into the apartment. As he entered, Detective Kershaw observed hanging on a vacuum cleaner a "very distinct" blue and yellow coat that was similar to the coat worn by the man with Ms. Jenkins in the surveillance videos. Once inside the apartment Detective Kershaw also observed several bottles of cleaning agents, a portion of the floor where the carpet had been ripped up, and bleach spots on the remaining carpet.

After some further conversation with the detectives at the apartment, Mr. Copes agreed to go to the police station. At the station, Mr. Copes was given *Miranda* warnings and spoke further with the police.[22]

---

the inhabitants of the other units in the building and determined that none of them were the man in the video.

[22] In an affidavit supporting a subsequently-issued search warrant, Detective Kershaw reported that Mr. Copes stated that he had known Ms. Jenkins for some time, but that she had never been inside his apartment.

Search Warrants

Early the next morning, February 19, 2014, Detective Kershaw applied to the District Court sitting in Baltimore City for a warrant to search Mr. Copes' apartment as well as a warrant to obtain a sample of Mr. Copes' DNA. Among the items retrieved during the search of the apartment were swabs of suspected blood that were later matched to Ms. Jenkins through DNA testing.

Some weeks later, upon reviewing the photos of Mr. Copes' apartment taken during the execution of the February 19, 2014 warrant, Detective Kershaw noticed a book sitting on Mr. Copes' desk in one of the photos. The title – *Spelling the Easy Way* – matched a library book that Ms. Jenkins had checked out of the Enoch Pratt Free Library shortly before her death. On April 7, 2014, Detective Kershaw applied for and obtained another search warrant for Mr. Copes' apartment. During the execution of this second warrant, the library book was retrieved from Mr. Copes' apartment.

C. Legal Proceedings

1. Charges

On March 31, 2014, Mr. Copes was indicted by a grand jury in Baltimore City and charged with first-degree murder and with wearing and carrying a dangerous weapon in violation of Maryland Code, Criminal Law Article, §4-101.

2. Motion to Suppress

Mr. Copes moved to suppress all evidence recovered from his apartment as well as his statements to police. He asserted that the Police Department's use of a cell site simulator was a warrantless and unreasonable search in violation of the Fourth Amendment

and that the evidence gathered as a result of the use of that device, including his identity and his statements to police, was the fruit of that illegal search.

The Circuit Court conducted a hearing on Mr. Copes' motion on April 25, 2016. At the hearing, Detective Haley and Detective Kershaw testified in detail about the techniques used by the Advanced Technical Team to track the -4686 cell phone to 4014 Penhurst Avenue. Both detectives also testified about the protocols followed in applying for the court order before the cell site simulator was used.

According to the detectives, the form of the application had been drafted and approved by the State's Attorney's Office and the Police Department's legal department, had been used since 2007, and was not revised until late 2014, after the investigation in this case. Detective Kershaw testified that he was not aware of any "issues" with the application, which had been used and approved "many, many times." In his experience, up through the time he applied for the orders at issue in this case, the application had, in fact, never been denied, nor had there "ever been any reservation expressed by [any judge of the Circuit Court for Baltimore City] as it relates to . . . the validity of those orders" obtained via the application.

Both detectives testified that they believed that the orders in this case authorized them to use the cell site simulator to locate the -4686 phone. Detective Haley said that he assumed that, if the judge to whom the application and draft order was presented had not thought them to be sufficient, the judge would not have signed the order. Although another detective had applied for the order in this case, Detective Haley testified that, had he been the one submitting the applications, he would have answered any of the judge's questions.

Detective Haley conceded that, at that time, there was a nondisclosure agreement between the Police Department and the FBI that ostensibly prevented disclosure of certain information about the cell site simulator.

Mr. Copes also testified briefly at the hearing to establish his standing to seek suppression of the evidence obtained through the cell site simulator. He stated that he was the owner of the -4686 phone. On cross-examination, he stated that he had let a "dear friend" named Ina use the phone.

3. Circuit Court Ruling

The Circuit Court granted Mr. Copes' motion to suppress. The court explained its reasoning in an oral opinion that relied heavily on the then-recent decision of the Court of Special Appeals in *State v. Andrews*, 227 Md. App. 350 (2016), that had affirmed a circuit court decision suppressing evidence derived from use of a cell site simulator.[23] The Circuit Court stated its belief that "these police officers acted in good faith" and noted some distinctions from the facts in *Andrews* – in *Andrews* the police used the device to find the known cell phone of a known suspect while in this case the suspect was unknown and the police believed the phone belonged to the victim. Nevertheless, the court felt bound to follow the decision in *Andrews*.

The Circuit Court also considered whether the police would have inevitably discovered Mr. Copes without use of the cell site simulator, and opined that "this case is a

[23] The *Andrews* decision is discussed in greater detail below. See Part II.B.2-3 of this opinion.

much closer call than *Andrews*." However, it reasoned that, even if the detectives had eventually found Mr. Copes at 4014 Penhurst Avenue, it might have been at a later time when the incriminating evidence in the apartment was gone. The court also rejected an argument that the pen register and other CSLI data (apart from the use of the cell site simulator) would have independently led the detectives to Mr. Copes, noting that the CSLI data "didn't pinpoint this particular location."

The court reiterated its finding that "these officers operated in good faith," but held that the use of the cell site simulator without a warrant was an unconstitutional search. As a result, it held that evidence derived from that search – all evidence seized from Mr. Copes' apartment as well as his statements to police – should be suppressed as fruit of an illegal search. The State appealed.

4. Appeal to Court of Special Appeals

In an unpublished opinion issued October 25, 2016, the Court of Special Appeals affirmed the Circuit Court ruling. Citing its previous decision in *Andrews*, the intermediate appellate court held that the use of the cell site simulator was a Fourth Amendment search and that the order based on the Pen Register Statute was not a constitutionally-sufficient authorization for that search. It also rejected the State's arguments as to why the exclusionary rule should not be applied. It held that the discovery of Mr. Copes – and the evidence in his apartment – was not inevitable or sufficiently attenuated from the use of the cell site simulator to avoid application of the exclusionary rule.[24] Similarly, it rejected

[24] Because the State did not raise an attenuation argument in the Circuit Court, the Court of Special Appeals held that this argument was waived on appeal. Nevertheless, the

the State's argument that the police officers believed, in good faith, that the order authorized the use of the cell site simulator, because, when applying for the order, they "did not provide clearly what technology [they] sought to use, nor the manner in which the technology operated."

The State petitioned this Court for a writ of *certiorari*, which we granted.

II

Discussion

A. Standard of Review

In reviewing a trial court's decision to grant or deny a motion to suppress evidence based on a constitutional violation, we generally accept any fact findings made by the trial court unless they are clearly erroneous. The ultimate question as to whether there was a constitutional violation is a legal question on which we accord no special deference to the trial court. *See Sinclair v. State*, 444 Md. 16, 27 (2015). Similarly, the application of the exclusionary rule – and whether there is an applicable exception to that rule in the particular case – is a question of law that we decide without deference to the lower court. *Marshall v. State*, 415 Md. 399, 408 (2010); *see also McDonald v. State*, 347 Md. 452, 470 n.10

---

intermediate appellate court concluded that, even if the State had preserved that argument, it would be unavailing because (1) the discovery of Mr. Copes in his apartment occurred shortly after the detectives used the cell site simulator, (2) Mr. Copes' decision to allow Detective Kershaw into his apartment was a direct result of the use of the cell site simulator, and (3) the Police Department and the State's Attorney's Office were operating under the nondisclosure agreement with the FBI, which the court viewed as an affirmative effort "to hide this technology from public and judicial oversight."

(1997) (ultimate question whether good faith exception to exclusionary rule applies is a legal issue).

B. Whether Evidence Obtained by Use of a Cell Site Simulator Should be Suppressed

The State presents one question for review: Did the lower courts err in excluding the evidence? The facial simplicity of this single question belies its multi-layered complexity. It can be broken down into three parts:

> (1) *Search* – Was use of the cell site simulator in this case a search for purposes of the Fourth Amendment?
>
> (2) *Warrant* – If use of the cell site simulator was a search, did the court order obtained by the police serve the function of a warrant for purposes of the Fourth Amendment?
>
> (3) *Exception to Suppression* – If the court order was not equivalent to a warrant, is there an applicable exception to the warrant requirement or to the exclusionary rule that allows for admission of the evidence at trial?

We shall not answer the first two questions. With respect to the first question, the State has conceded, for purposes of this case, that the use of the cell site simulator constituted a search. There is no reason to deviate from the usual rule against providing an advisory opinion in order to give a definitive answer to that question, particularly when the issue concerns a rapidly changing technology and shifting legal landscape.

The State does ask us to answer the second question as to the sufficiency of the court order as a warrant for purposes of the Fourth Amendment. This, however, is a close question – and one that is not likely to recur, at least with respect to the format of this particular order. As noted earlier, the General Assembly enacted a statute three years ago that specifically addresses court orders authorizing law enforcement use of devices such as

cell site simulators. Presumably any orders issued in the interim have been based on that statute. In any event, it is not necessary to answer this question to resolve this case.

We will answer the third question. In particular, we will decide whether the good faith exception to the exclusionary rule applies in these circumstances, even if one considers use of the cell site simulator to locate a cell phone to be a search and the court order in this case inadequate as a warrant. In doing so, we will discuss factors bearing on each of the first two questions, as they affect the assessment of whether the good faith exception applies here. For the reasons set forth below, we conclude that it does.[25]

1. The Exclusionary Rule and the Good Faith Exception

The Fourth Amendment to the United States Constitution states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[26] To vindicate this guarantee and deter violations by law enforcement, the Supreme Court has developed the "exclusionary rule." Under the exclusionary rule, evidence obtained in violation of the Fourth Amendment is ordinarily excluded from the criminal trial of a defendant whose rights were violated by an

[25] Because our resolution of this case turns on the good faith of the officers, we need not – and do not – address the State's arguments on inevitable discovery and attenuation.

[26] This Court has held that the Maryland Constitution provides the same protection in Article 26 of the Maryland Declaration of Rights. *See Givner v. State*, 210 Md. 484 (1956); *see also* D. Friedman, The Maryland State Constitution: A Reference Guide (2006) 36-37.

illegal search or seizure. *Weeks v. United States*, 232 U.S. 383 (1914) (establishing the exclusionary rule in federal courts); *Mapp v. Ohio*, 367 U.S. 643 (1961) (extending exclusionary rule to state courts).

The exclusionary rule is not itself an individual right; therefore, suppression of evidence "is not an automatic consequence of a Fourth Amendment violation." *Herring v. United States*, 555 U.S. 135, 137, 141 (2009). The Supreme Court has cautioned that suppression "has always been our last resort, not our first impulse." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). The rule's sole purpose is to deter future Fourth Amendment violations by law enforcement. *United States v. Leon*, 468 U.S. 897, 916 (1984). It is to be applied only when this "deterrent effect [is] substantial and outweigh[s] any harm to the justice system." *Herring*, 555 U.S. at 147; *see also United States v. Calandra*, 414 U.S. 338, 348 (1974). Because the rule imposes a "costly toll upon truth-seeking and law enforcement objectives," those arguing for its application face a "high obstacle." *Pennsylvania Bd. Of Probation and Parole v. Scott*, 524 U.S. 357, 364 (1998) (internal quotations and citations omitted).

The exclusionary rule is not applied when law enforcement officials engage in "objectively reasonable law enforcement activity," even if that activity is later found to be a violation of the Fourth Amendment. *Leon*, 468 U.S. at 919. This exception to the exclusionary rule is also known as the "good faith exception" because it depends on whether law enforcement officers acted in good faith. *Davis v. United States*, 564 U.S. 229, 238 (2011). For example, the Supreme Court has held the good faith exception applicable when law enforcement officers (1) conducted a search pursuant to a facially

valid search warrant that was later found to lack probable cause,[27] (2) conducted a search pursuant to a statute authorizing warrantless administrative searches that was later held to be unconstitutional,[28] (3) made an arrest pursuant to a warrant listed in a judicially-maintained database that was later revealed to be inaccurate because the warrant had been quashed,[29] (4) made an arrest pursuant to a warrant listed in a law enforcement-maintained database that was later revealed to be inaccurate because the warrant had been recalled,[30] and (5) conducted a search in reliance on binding appellate precedent that was later overruled.[31] This Court has applied the good faith exception in similar circumstances.[32]

The Supreme Court has described four situations in which the good faith exception would not be applied: (1) the magistrate is misled by information in the application for the warrant that the officer knew was false or would have known was false, except for a reckless disregard for the truth; (2) the magistrate wholly abandons a detached and neutral role; (3) the affidavit is so lacking in probable cause so to render official belief in its

---

[27] *Leon*, 468 U.S. 897.

[28] *Illinois v. Krull*, 480 U.S. 340 (1987).

[29] *Arizona v. Evans*, 514 U.S. 1 (1995).

[30] *Herring v. United States*, 555 U.S. 135 (2009).

[31] *Davis v. United States*, 564 U.S. 229 (2011).

[32] *See, e.g.*, *Spence v. State*, 444 Md. 1, 10-13 (2015) (applying good faith exception where law enforcement officers conducted a search in reliance on binding appellate precedent that was later overruled); *Patterson v. State*, 401 Md. 76, 104-11 (2007) (applying good faith exception when law enforcement officers conducted a search pursuant to a facially valid search warrant that was later found to lack probable cause).

existence entirely unreasonable; (4) the warrant is so facially deficient, by failing to particularize the place to be searched or the things to be seized, that the executing officers cannot reasonably presume it to be valid.[33]

Relevant to the application of the good faith exception here – and whether the suppression of evidence under the exclusionary rule would deter future unlawful conduct by investigators – is the extent to which it should have been clear to the detectives in this case (1) that the courts would determine that use of a location tracking device like the cell site simulator was a search and (2) that a court order in the format similar to that used for pen registers and trap and trace orders would be inadequate to authorize use of the device.

2. Location Tracking and Fourth Amendment Searches

Two basic principles governing application of the Fourth Amendment are that it "protects people, not places"[34] and that a "Fourth Amendment search occurs [only] when the government violates a subjective expectation of privacy that society recognizes as reasonable."[35] The Supreme Court has reached varying conclusions about the application of these principles to the use of location tracking devices, and has recently agreed to consider such an issue related to cell phones. A number of lower courts have discussed the Fourth Amendment implications of location tracking by means of CSLI and cell site simulators.

---

[33] *Leon*, 468 U.S. at 923; *see also Patterson v. State*, 401 Md. 76, 104 (2007).

[34] *Katz v. United States*, 389 U.S. 347, 352 (1967).

[35] *Kyllo v. United States*, 533 U.S. 27, 33 (2001).

a. Real-Time Location Tracking Not Involving Cell Phones

Beepers – to the home v. in the home

In a pair of cases from the 1980s involving then-contemporary technology, the Court reached different conclusions on whether the clandestine use of a radio transmitter – a "beeper" – by law enforcement officers to track a suspect or contraband in the suspect's control constituted a search for purposes of the Fourth Amendment. The difference appeared to turn on whether the device tracked movement in a public place or within a private dwelling.

In one case,[36] law enforcement officers installed a beeper in a container of chemicals purchased by the suspect and then tracked the container as the suspect transported it via automobile to the area around a cabin where he operated a drug laboratory. The Court held that the use of the beeper was not a Fourth Amendment search. The Court observed that, by travelling over the public streets, the suspect "voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction," and that the beeper was not used to reveal information as to the movement of the container within the cabin. The Court concluded that the suspect had no reasonable expectation of privacy in the container's movements.[37]

[36] *United States v. Knotts*, 460 U.S. 276, 277-79 (1983).

[37] *Knotts*, 460 U.S. at 281, 285. The defendant did not challenge the physical installation of the beeper, only its tracking by law enforcement. *Id*. at 279, n.**.

In the other case,[38] law enforcement officers installed a beeper in a container of chemicals purchased by the suspect and again tracked the container, this time *into* – and not just to the area around – a home. Unlike the previous case, where the beeper "told the authorities nothing about the interior of [the] cabin," the Court noted that the tracking in the second case indicated that the beeper was inside the suspect's house, "a fact that could not have been visually verified."[39] Because individuals have privacy interests in their homes, the Court concluded that this tracking was a Fourth Amendment search.[40]

GPS trackers – trespass v. reasonableness

Nearly 30 years later, the Court considered law enforcement use of a Global Positioning System (GPS) device to track a suspect for an extended period of time. In that case,[41] law enforcement officers attached a GPS device to the suspect's automobile and tracked the vehicle's movements for 28 days. The Court unanimously agreed that these actions constituted a Fourth Amendment search, but the justices differed on the rationale for this conclusion. A majority of five justices attributed the violation to the fact that the officers had committed a common law trespass when they installed the device on the car.[42] The majority opinion declined to delve into the "thorny problems" that might be posed if

---

[38] *United States v. Karo*, 468 U.S. 705, 707-10 (1984).

[39] *Id.* at 715.

[40] *Id.* at 718.

[41] *United States v. Jones*, 565 U.S. 400, 402-03 (2012).

[42] *Id.* at 404-07 (Scalia, J.) (concluding that the government "physically occupied private property for the purpose of obtaining information").

the tracking involved only the transmission of electronic signals, but noted that such a case would be subject to a reasonableness analysis.[43] The other four justices would have resolved the case by applying a reasonableness test under which short-term monitoring of movements on a public street by means of a GPS device would be reasonable as in "accord with expectations of privacy that our society has recognized as reasonable" while longer term monitoring would violate those expectations.[44] Two concurring opinions in *Jones* predicted that advances in personal technology would enhance location tracking capabilities, affect expectations of privacy, and raise additional questions under the Fourth Amendment.[45]

b. Retrospective Location Tracking via Cell Phone – Historical CSLI

As described earlier in this opinion, the location of a cell phone can be approximated by analyzing service provider records of the cell towers with which the phone connected

---

[43] *Id.* at 411-13.

[44] 565 U.S. at 418-30 (Alito, J., concurring in the judgment).

[45] Writing for four justices, Justice Alito noted that "cell phones and other wireless devices now permit wireless carriers to track and record the location of users" without a physical trespass; that such features are offered to and desired by consumers; and that "the availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements." 565 U.S. at 428-29 (Alito, J., concurring in the judgment).

In a separate concurrence, Justice Sotomayor, who joined the five-justice majority subscribing to the trespass theory, warned that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." She nevertheless conceded that "the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations." 565 U.S. at 415 (Sotomayor, J., concurring).

to make and receive calls and text messages. Appellate courts have reached different conclusions as to whether the warrantless collection of historical CSLI implicates the Fourth Amendment. The United States Supreme Court recently agreed to consider whether a search warrant is required for law enforcement officers to obtain historical CSLI from a service provider. *United States v. Carpenter*, ___U.S. ___, 2017 WL 2407484 (June 5, 2017).

Most courts have concluded that law enforcement access to historical CSLI is not a search for purposes of the Fourth Amendment. They have cited the "third party doctrine," which the Supreme Court elucidated in concluding that law enforcement officers do not conduct a search for purposes of the Fourth Amendment when they request a telephone company to install a pen register[46] or obtain a depositor's bank records from a financial institution.[47] For example, in *United States v. Graham*, 824 F.3d 421, 427 (2016) (*en banc*), the Fourth Circuit concluded that an individual does not have a reasonable expectation of privacy in a cell phone's historical CSLI. The Fourth Circuit reasoned that, because a cell phone user voluntarily shares that information with third parties – *i.e.*, cell phone service providers – whenever the cell phone user makes a call or sends a text message, the user cannot reasonably expect it to remain private. 824 F.3d at 427-28. Accordingly, the collection of such data by law enforcement officers is not a Fourth Amendment search.

[46] *Smith v. Maryland*, 442 U.S. 735 (1979); see Part I.A.2 of this opinion above.

[47] *United States v. Miller*, 425 U.S. 435 (1976).

Many other federal appellate courts have come to the same conclusion as the Fourth Circuit in *Graham* based on the same reasoning. *See, e.g., United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert granted*, ___U.S. ___, 2017 WL 2407484 (June 5, 2017); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (*en banc*); *In re application of the United States for historical cell site data*, 724 F.3d 600 (5th Cir. 2013); *see Graham*, 824 F.3d at 428-29 & nn.6-7 (collecting cases); *see also Zanders v. Indiana*, 73 N.E.3d 178 (Ind. 2017).

The Third Circuit, however, has reached a different conclusion, and rejected application of the third party doctrine to historical CSLI. *In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304, 317 (3rd Cir. 2010). In that case, the court reasoned that a cell phone user does not share location information with a service provider "in any meaningful way." Nevertheless, that court held that federal law enforcement officers need not demonstrate probable cause – the standard for obtaining a search warrant – in order to obtain historical CSLI. Rather, the officer need only make a showing required by the federal Stored Communications Act – that is, "specific and articulable facts showing that there are reasonable grounds to believe that [the historical CSLI is] relevant and material to an ongoing investigation." *Id.* at 315 (citing 18 U.S.C. §2703(d)); *see also In re Application of the United States for an Order Authorizing the Release of Historical Cell Site Information*, 809 F.Supp.2d 113 (E.D.N.Y. 2011) (holding that third party doctrine does not apply to historical CSLI).

The Massachusetts Supreme Judicial Court has also rejected the third party doctrine with respect to historical CSLI and, construing its state constitutional analog to the Fourth Amendment, has looked to the duration of the location tracking to assess whether the cell phone user has a reasonable expectation of privacy in historical CSLI. *See Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014) (holding that law enforcement access to historical CSLI for a two-week period is a search under state constitutional provision, although a warrant may not be needed for a period of shorter duration); *Commonwealth v. Estabrook*, 38 N.E.3d 231 (Mass. 2015) (confirming that law enforcement officers may obtain historical CSLI relating to a period of six hours or less without need for a search warrant).

c. Real-Time Location Tracking via Cell Phone

Real-time tracking of the location of a cell phone – and, presumably the cell phone's owner or user – can occur via data from the cell phone's GPS, via information about the cell towers currently being utilized by the cell phone (*i.e.*, real-time CSLI), and – as in this case – via the use of a cell site simulator. As with historical CSLI, the courts have reached different conclusions as to whether such real-time tracking is a search for purposes of the Fourth Amendment and the Supreme Court has not yet had occasion to analyze the issue.

GPS data

In *United States v. Skinner*, 690 F.3d 772, 774-76 (6th Cir. 2012), *cert. denied,* 133 S.Ct. 2851 (2013), law enforcement officers located the defendant at a roadside truck stop

by tracking, in real time and without a warrant, GPS data broadcast by his cell phone.[48] The Sixth Circuit, noting that the defendant was "traveling on a public road before he stopped at a public rest stop," held that the defendant had no reasonable expectation of privacy in the location of his cell phone. *Id.* at 778. Moreover, the tracking took place over three days, which the court characterized as the "relatively short-term monitoring" that four justices in *Jones* had believed to be reasonable. Therefore, in the Sixth Circuit's view, the collection of such data is not a Fourth Amendment search.

Real-time CSLI

In *Tracey v. State*, 152 So.3d 504, 506-07 (Fla. 2014), law enforcement officers located the defendant by tracking, in real time and without a warrant, his cell phone's real-time CSLI. The Florida Supreme Court, emphasizing that real-time – and not historical – CSLI was at issue, held that a cell phone user has a reasonable expectation of privacy in such data, "even on public roads." *Id.* at 516, 526. Therefore, in that court's view, the collection of that data was a Fourth Amendment search.[49] *See also In re Application of the United States for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone*, 849 F.Supp.2d 526 (D. Md. 2011) ("the subject here has a reasonable

[48] Law enforcement officers also utilized real-time CSLI, but the defendant apparently did not challenge the use of that data on Fourth Amendment grounds. *Skinner*, 690 F.3d at 776-77.

[49] The court also rejected the state's reliance on the third party doctrine, noting that "[s]imply because the cell phone user knows or should know that his cell phone gives off signals that enable the service provider to detect its location for call routing purposes ... does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes." *Tracey*, 152 So.3d at 522.

expectation of privacy both in his location as revealed by real-time location data [*i.e.*, CSLI] and in his movement where his location is subject to continuous tracking over an extended period of time, here thirty days"); *but see In re Application of the United States for an Order for the Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace Device*, 405 F.Supp.2d 435 (S.D.N.Y. 2005) (holding, pursuant to the third party doctrine, that the collection of certain real-time CSLI is not a Fourth Amendment search).

Cell Site Simulator

In *United States v. Patrick*, 842 F.3d 540, 541 (7th Cir. 2016), law enforcement officers located and arrested the defendant – for whom they had a valid arrest warrant – in a car on a public street with the assistance of a cell site simulator. Although the officers had obtained a warrant to track the defendant through cell phone data, the application for the warrant did not specifically inform the issuing magistrate that a cell site simulator would be used. 842 F.3d at 542, 544. The defendant argued that the warrant was invalid and that evidence found on his person at the time of his arrest should be suppressed. *Id.* at 541. The Seventh Circuit disagreed. Because the defendant was in a public place at the time of the arrest and because "probable cause alone is enough for an arrest in a public place," the court held that the defendant "did not have any privacy interest in his location

at the time" and "[could not] complain about how the police learned his location." *Id.* at 542, 545.[50]

In *Patrick*, as in this case, the government conceded for purposes of that case that use of the cell site simulator was a Fourth Amendment search. The court's conclusion that the defendant "did not have any privacy interest in his location at the time" seems to imply – at least under *Katz* – that it would not be a search, so long as the defendant was tracked in a public place. In any event, the court demurred on resolving that question in the case before it:

> Questions about whether use of a [cell site] simulator is a search, if so whether a warrant authorizing this method is essential, and whether in a particular situation a [cell site] simulator is a reasonable means of executing a warrant, have yet to be addressed by any United States court of appeals. We think it best to withhold full analysis until these issues control the outcome of a concrete case.

842 F.3d at 545. *But see United States v. Lambis,* 197 F.Supp.3d 606, 611(S.D.N.Y. 2016) (use of cell site simulator is search for purposes of Fourth Amendment).

d. The *Andrews* Case

As noted above, the Court of Special Appeals has had occasion to consider whether law enforcement use of a cell site simulator is a search for purposes of the Fourth Amendment in *State v. Andrews*, 227 Md. App. 350 (2016). The *Andrews* decision concerned events roughly contemporaneous with those in this case. The opinion was

[50] The court noted that the cell site simulator was not used to generate the probable cause for the arrest of the defendant, only to find his location. 842 F.3d at 545 ("A fugitive cannot be picky about how he is run aground.").

issued shortly before the Circuit Court's ruling in this case and was relied upon the Circuit Court.

In *Andrews*, the defendant had been charged with first-degree murder related to a shooting during an illicit drug transaction. A warrant was issued for his arrest, but police were initially unable to locate him. Officers learned the number of the defendant's cell phone through a confidential informant. The officers applied for – and obtained – a court order based in part on the Pen Register Statute, similar to the order in this case. Using a cell site simulator, officers were able to locate the cell phone – and the defendant – at a home in Baltimore. They arrested the defendant and then obtained a search warrant for the home where they found a gun in the cushions of the couch where the defendant had been sitting. The circuit court granted the defendant's motion to suppress the gun and other evidence as fruits of an illegal search – *i.e.*, the use of the cell site simulator without a search warrant.[51]

The Court of Special Appeals upheld the circuit court's decision in a comprehensive opinion. After an extensive review of the case law and legal literature, the intermediate appellate court concluded that cell phone users have an objectively reasonable expectation that the users' cell phones "will not be used as real-time tracking devices through the direct and active interference of law enforcement." 227 Md. App. at 394-95. It rejected application of the third party doctrine, noting that the particular data intercepted by the cell

[51] Unlike this case, the circuit court did not conduct a full-fledged hearing on the motion to suppress but, with the consent of the parties, held a truncated hearing that incorporated testimony from a hearing concerning a discovery dispute.

site simulator had never been transmitted to a service provider. *Id.* at 398-99.[52] Consequently, it held that the officers' use of a cell site simulator to locate the defendant was a search for purposes of the Fourth Amendment.

e. Summary

It is evident that, in assessing whether law enforcement use of location tracking data and devices is a search for purposes of the Fourth Amendment, courts have looked to a variety of factors – whether use of a device involves a physical trespass, whether the device is used for long-term or short-term tracking, whether the device tracks movements within a private dwelling or on a public street, and whether the information conveyed is also knowingly shared with a third party. In this case, some of those factors – the short duration of tracking, its use in this case to identify a building rather than movements within the building, and the absence of any physical trespass – favor a conclusion that use of the device to find the -4686 phone was not a search.

On the other hand, as the Court of Special Appeals observed in *Andrews*, a cell site simulator provides law enforcement officers with information not originally collected by the service provider and, thus, there is a strong argument that the third party doctrine does not apply. Moreover, depending on the precision of the particular device, it may have the capability of providing detailed information about movements within a dwelling.

---

[52] In that regard, the court also relied on the panel decision in *United States v. Graham*, 796 F.3d 332, 355-56 (4th Cir. 2015), which rejected the third party doctrine and held that law enforcement access to historical CSLI was a search. Two months after the Court of Special Appeals decided *Andrews*, that decision was overruled by the Fourth Circuit sitting *en banc*. *United States v. Graham*, 824 F.3d 421 (2016) (*en banc*).

One of the key cases relied upon in *Andrews* has since been overruled by the Fourth Circuit *en banc*.[53] Moreover, the Supreme Court has now agreed to take up the question whether law enforcement access to CSLI implicates the Fourth Amendment[54] and thus there may be a decision in the near future providing authoritative guidance for that closely-related issue. None of this means that the analysis in *Andrews* is wrong. Indeed, the analysis in *Andrews* and the other cases summarized above may well prove useful when we inevitably must consider the use of a cell site simulator pursuant to the General Assembly's recently-enacted statute. But, given that the State has conceded for purposes of this case that use of the cell site simulator was a search, it seems "best to withhold full analysis until these issues control the outcome of a concrete case."[55]

In any event, for purposes of the question whether the detectives in this case acted in objectively reasonable good faith, it is enough to note that the holding of the Court of Special Appeals post-dated the use of the cell site simulator in this case by two years, and the case law in other jurisdictions concerning real-time location tracking did not make it a foregone conclusion that use of a cell site simulator would be considered a search in all instances under the Fourth Amendment.

---

[53] See footnote 51.

[54] *United States v. Carpenter*, ___ U.S.___, 2017 WL 2407484 (June 5, 2017).

[55] *Patrick*, 842 F.3d at 545; *see also City of Ontario, Cal. v. Quon*, 560 U.S. 746, 759 (2010) ("[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear").

3. Court Order as Equivalent to Warrant

The Fourth Amendment's prohibition against unreasonable searches is generally satisfied when law enforcement officers obtain a warrant authorizing the search in question. *Riley v. California*, 134 S.Ct. 2473, 2482 (2014).[56] Here, the State contends that the order obtained by the officers based in part on the Pen Register Statute functioned as constitutionally-sufficient authorization for the use of the cell site simulator – in other words, it was a warrant for purposes of the Fourth Amendment.

a. Requirements for a Warrant

In order to obtain a search warrant, a law enforcement officer must demonstrate probable cause in sworn testimony presented to a "neutral and detached magistrate." *Illinois v. Gates*, 462 U.S. 213, 238-240 (1983). "Probable cause," in turn, is "a fair probability that contraband or evidence of a crime will be found in a particular place," *id.*, or a showing "that the evidence sought will aid in a particular apprehension or conviction for a particular offense," *Dalia v. United States*, 441 U.S. 238, 255 (1979). As for the Fourth Amendment's particularity requirement, although the Supreme Court has not had to squarely rule on how it applies to real-time location tracking, the Court suggested that, in the context of location tracking by electronic beeper, it would be sufficient for law

[56] Searches may also be constitutionally "reasonable" if there is an applicable exception to the warrant requirement. *Riley*, 134 S.Ct. at 2482. One such exception covers searches conducted with the individual's consent. *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973). In the Circuit Court, the State claimed that Mr. Copes consented to the search of his apartment. The State, however, did not raise this argument in the Court of Special Appeals or this Court. Therefore, we do not address it.

enforcement officers applying for a warrant to "describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested."[57]

b. Warrants for Location Tracking with Cell Site Simulator

Two federal district court decisions illustrate the specificity that may be required for a warrant authorizing the use of a cell site simulator to locate or track a suspect. In both cases, law enforcement officers obtained a warrant for location tracking and used a cell site simulator, and in both cases the defendant later asserted that the use of the cell site simulator exceeded the scope of the warrant. In one case, the officers notified the court in the application that they intended to use a "mobile tracking device." In the second case, the officers did not. The court denied the motion to suppress in the first case, but granted it in the second case.

In *United States v. Ringmaiden*, 2013 WL 1932800 (D. Ariz. 2013), law enforcement officers obtained a warrant authorizing the "use and monitoring of a mobile tracking device" in order to track an "aircard" in the defendant's computer. The aircard, which allowed the defendant's computer to wirelessly connect to the internet through a service provider's cell towers, was identified in the warrant by its assigned phone number and device serial number. *Id.* at *14. After it was revealed that the officers used a cell site simulator to track the aircard, the defendant moved to suppress evidence gathered as a result of that tracking. He argued, among other things, (1) that use of a cell site simulator

[57] *Karo*, 468 U.S. at 718.

exceeded the scope of the warrant because it was not specifically authorized by the warrant, and (2) that the warrant lacked particularity, because it did not describe the place to be searched.

The federal district court rejected those arguments. Holding that the use of a cell site simulator did not exceed the scope of the warrant, the court first noted that "[t]here is no legal requirement that a search warrant specify the precise manner in which the search is to be executed." *Id.* at *16. The court reasoned that the warrant's reference to a "mobile tracking device" reasonably described the equipment used to track signals from the aircard – *i.e.*, the cell site simulator. *Id.* at *17. In finding that the warrant was sufficiently particular, the court observed that a warrant to locate a particular item need not specify the place to be searched, if the warrant provides other information. *Id.* at *22. In the case before the court, the particularity requirement was satisfied as the warrant precisely identified the aircard to be located by description, telephone number, and device serial number. *Id.* at *17, 22.

By contrast, in *United States v. Lambis*, 197 F.Supp.3d 606 (S.D.N.Y. 2016), officers obtained a warrant to track a suspect via CSLI for a target phone.[58] The application for the warrant made no mention of a "cellular tracking device," much less a cell site simulator. As in the instant case, the officers first used CSLI to determine the

[58] It is not clear from the opinion whether the warrant authorized the collection of historical or real-time CSLI. However, the law enforcement officers apparently used the CSLI to identify the phone's location after the warrant was issued, which presumably would be real-time CSLI.

phone's general vicinity and then used a cell site simulator to pinpoint the phone to a specific apartment within an apartment building. The court suppressed the evidence discovered in that apartment on the ground that the use of the cell site simulator exceeded the scope of the search permitted by the warrant. The court opined that, because the government was able to demonstrate probable cause to obtain a warrant for CSLI, it could have also obtained a warrant to use a cell site simulator, if it had wished to do so.

c. Orders Based on Pen Register Statute

As noted earlier, many law enforcement agencies, like the detectives in this case, have sought court authorization to use cell site simulators through applications and orders based in part on a pen register statute. Unlike a search warrant, there is no requirement that there be a showing of probable cause as a predicate to an order under a pen register statute. However, as in this case, many such applications related to use of cell site simulators have purported to make some showing of probable cause.

Using Real-Time CSLI Pursuant to Order Based on Pen Register Statute

In *United States v. Wilford,* 961 F.Supp.2d 740, 744 (D. Md. 2013), law enforcement officers obtained an order based in part on the Maryland Pen Register Statute and proceeded to "ping"[59] the defendant's cell phone in order to generate real-time CSLI. The

[59] As noted above, a cell phone reveals its general geographical location whenever it sends or receives a call or text message. If one "pings" a cell phone – that is, sends signals to the phone – the phone may reveal its general geographical location at frequent, predictable intervals. *United States v. Wilford*, 961 F.Supp.2d 740, 747 (citing Susan Friewald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 702-03 (2011)). In *Wilford*, law enforcement officers pinged the defendant's phone every 15 minutes. 961 F.Supp.2d at 747.

court assumed that the pinging constituted a Fourth Amendment search and that such surveillance was not "embraced" by the Pen Register Statute. Nevertheless, it held that the order satisfied the Fourth Amendment's warrant requirement. 961 F.Supp.2d at 770-72. The court stated that it was immaterial that the order was not titled as a "warrant" and looked to the substance of the order and supporting application. *Id.* at 773. The court noted that the application was submitted under oath, identified a specific cell phone, and "generally provided adequate information obtained through the investigation to establish probable cause." *Id.* at 772-73.

In a case in which the officers provided less detail in an application for an order based on a pen register statute, the Florida Supreme Court reached a different result. *Tracey v. Florida,* 152 So.3d 504 (Fl. 2014). In order to satisfy the relevance standard of the pen register statute, the application for the order noted merely that a confidential informant told law enforcement that the defendant (1) transports drugs from one location to another and (2) uses a certain cell phone number. The application did not seek authority to track the location of the defendant's cell phone, nor did it seek access to real-time CSLI. Nevertheless, the officers used real-time CSLI to track the defendant inside a private home. The court held that the information provided in the application did not amount to probable cause and that the order, therefore, did not provide constitutionally-sufficient authorization for the location tracking. *See also In re Application of the United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F.Supp.2d 816

(S.D. Texas 2006) (denying application for order submitted under 18 U.S.C. §3121 that sought authorization for the collection of CSLI).

Using Cell Site Simulator Pursuant to Order Based on Pen Register Statute

In a case with facts very similar to this case, the Wisconsin Supreme Court assumed that law enforcement use of a cell site simulator is a search for purposes of the Fourth Amendment and that a warrant would be required because use of the cell site simulator led to the defendant's apprehension in a private dwelling. That court concluded that an order based on the state pen register statute sufficed as a warrant in light of the content of the application for that order and the order itself. *Wisconsin v. Tate*, 849 N.W.2d 798 (Wis. 2014), *cert. denied*, 135 S.Ct. 1166 (2015).

In *Tate*, officers were investigating a murder that occurred outside a grocery store. Surveillance camera footage from the store showed the murderer purchasing a prepaid cell phone from the store shortly before committing the crime. The police obtained identifying information about the phone, and obtained an order based on the Wisconsin pen register statute, which is similar in pertinent respects to the Maryland statute. The application for the order summarized the facts of the investigation and the purpose in tracking the cell phone. The order authorized the officers to obtain not only information provided by a pen register, but also CSLI from the service provider, as well as GPS location information and "the identification of the physical location of a target cellular phone." 849 N.W.2d at 802 n.6. As in this case, the officers then used a cell site simulator in combination with CSLI in order to locate the phone within a specific apartment building. *Id.* at 804. The officers

canvassed the apartments in the building, eventually finding the individual from the grocery store video in one of the apartments. *Id*.

In holding that the trial court properly denied the defendant's motion to suppress evidence and statements, the Wisconsin Supreme Court held that the order functioned as a warrant for purposes of the Fourth Amendment and that the officers' use of the cell site simulator was not an unreasonable search. *Id.* at 801 & n.3. The court noted that the application for the order described sufficient facts to support a finding of probable cause, even though the Wisconsin statute, like the Maryland Pen Register Statute, required only a showing that the information sought would be relevant to an ongoing criminal investigation. In addition, it held that the order was sufficiently particular because it identified a particular phone and "permit[ted] a particularized collection of cell site information for only [that] phone." *Id.* at 810.

As noted above, in *Andrews*, the police obtained an order – similar to the order in this case – under the Maryland Pen Register Statute. The Court of Special Appeals concluded that the order did not suffice as a warrant in that case. The court compared the functionality of a pen register and trap and trace device to the functionality of a cell site simulator. It also looked to federal court decisions holding that the government was not entitled to obtain real-time CSLI under the federal pen register statute without a showing of probable cause[60] and a federal court decision declining to issue such an order with

[60] *In re Application of the United States for an Order Authorizing Installation & Use of a Pen Register*, 415 F.Supp.2d 211 (W.D.N.Y. 2006); *In re Application for Pen*

respect to a cell site simulator.[61] The court also noted that, unlike the standards for a search warrant, the Pen Register Statute does not require a showing of probable cause, nor does it contain a particularity requirement.[62] The intermediate appellate court concluded that the Pen Register Statute was limited in its reach and not intended to apply to "other, newer technologies." 227 Md. App. at 406. Finally, the court stated that the order was not "based on sufficient information about the technology to allow [the issuing] court to contour reasonable limitations on the scope and manner of the search" and did not "provide[] adequate protections in case any third-party cell phone information might be unintentionally intercepted." *Id.* at 413.[63]

Register &Trap/Trace Device with Cell Location Auth., 396 F.Supp.2d 747 (S.D. Tex. 2005).

[61] *In the Matter of the Application of the United States for an Order Authorizing the Installation and Use of Pen Register and Trap and Trace Device*, 890 F.Supp.2d 747 (S.D. Tex. 2012).

[62] The court contrasted the showing required under the Pen Register Statute with the stricter showing required under the statute that now governs real-time location tracking through cell phones. 227 Md. App. at 406-7. That statute is described briefly in Part I.A.3 of this opinion above.

[63] The court related the perceived lack of detail to a nondisclosure agreement between the FBI and the State's Attorney's Office concerning cell site simulators. The nondisclosure agreement stated that use of the equipment "shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including ... during judicial hearings." 227 Md. App. at 374. It also stated that the Police Department "shall not, in any civil or criminal proceeding, use or provide any information concerning the [equipment] ... during pre-trial matters, in search warrants and related affidavits ... without the prior written approval of the FBI." *Id.* at 374-75. In the view of the Court of Special Appeals, the agreement rendered the application for the order misleading and the resulting order "overreaching."

d. Summary

There is significant support in the case law for the position that an order under a pen register statute that is modified appropriately may function as a warrant for purposes of the Fourth Amendment. This is true when, in addition to being sworn, the application for the order demonstrates probable cause, and the order satisfies the particularity requirement of the Fourth Amendment. When these criteria are met, it does not matter whether the order is labeled a "warrant." The constitutional requirements are addressed to substance, not form.

In this case, the detectives submitted to the court a sworn application[64] based on the Pen Register Statute that purported to provide probable cause by summarizing evidence they had developed concerning the crime under investigation. In particular, the application identified a particular cell phone by number that was linked to the victim of the crime, but not found with her body. The application detailed the basis for the belief that location of the cell phone would lead to apprehension of the murderer. It requested authorization for "interception of real-time cell site information." The resulting order was issued by a "neutral magistrate" (a circuit court judge), stated that "the Court finds that probable cause

[64] Mr. Copes has suggested that the order was not a sworn document because the detective submitting the application refers to himself as "your applicant" and the application at various place indicates that he "states" or "offers" information. This ignores the fact that the detective also uses the verb "certify" and the signature page indicates that the application was "sworn," although the date is missing. Moreover, there is no question that the application and order are based on the requirements of the Pen Register Statute which provides for applications under oath or affirmation. Mr. Copes has not provided sufficient evidence to defeat the "presumption of regularity" that normally attaches to court proceedings. *Black v. State*, 426 Md. 328, 337 (2012).

exists," identified a specific cell phone to be tracked, and authorized the actions requested in the application.

Nevertheless, we need not decide whether the order did, in the end, provide constitutionally-sufficient authorization for law enforcement use of the cell site simulator in this case. We recognize the strength the State's argument on this issue, however, because it is relevant to the analysis whether it is appropriate to apply the good faith exception to the exclusionary rule in this case.

4. Whether the Good Faith Exception Applies

In our view, the detectives investigating the murder of Ms. Jenkins were engaged in "objectively reasonable law enforcement activity" when they used the cell site simulator pursuant to the order based on the Pen Register Statute. According to Detective Kershaw, applications for similar orders had been approved "many, many times," and never denied. On their face, the application and order likely satisfy the requirements for a warrant that complies with the Fourth Amendment. There is a strong – perhaps even conclusive – argument that the order obtained under the Pen Register Statute provided constitutionally-sufficient authorization for use of the cell site simulator. Both Detective Haley and Detective Kershaw testified that they believed that the order authorized them to use the cell site simulator.

The Circuit Court reiterated twice that it believed that the detectives investigating Ms. Jenkins' murder were "operat[ing] in good faith" when they used the cell site simulator pursuant to a court order in order to locate the suspect. Indeed, at the conclusion of the motions hearing, the court complimented Detective Kershaw on his "fine work" in the case.

Yet in suppressing the evidence obtained in that investigation, the court appeared to believe, without articulating it, that the use of the cell site simulator foreclosed any application of the good faith exception.

In its opinion in this case, the Court of Special Appeals did explicitly address the good faith exception and concluded that it did not apply, reasoning that application for the order "did not provide clearly what technology it sought to use, nor the manner in which the technology operated." In doing so, the court referred not to the record of this case, but to a passage in *Andrews* concerning the nondisclosure agreement between the FBI and the State's Attorney's Office. To the extent that the *Andrews* decision is interpreted as a categorical denial of a good faith exception when police used a cell site simulator pursuant to a court order based on the Pen Register Statute, we reject such an interpretation.[65]

None of the reasons identified by the Supreme Court or this Court for discounting law enforcement reliance on an apparently valid warrant apply here. There is no allegation that the issuing judge "abandon[ed] a detached and neutral role" or that the detectives provided knowingly false information. Nor can it be said that probable cause was so lacking as "to render official belief in its existence entirely unreasonable" or that it was

[65] The *Andrews* decision did not explicitly consider whether the good faith exception applied to the use of the cell site simulator in the case before it. It did consider whether the State could rely on the good faith exception to save from suppression the evidence that was recovered pursuant to a search warrant following use of the cell site simulator. It concluded that the search warrant was tainted by the illegal search conducted with the cell site simulator. 227 Md. App. at 417-21.

"facially deficient" with respect to the particularity requirement.[66] *See Leon*, 468 U.S. at 923.

The alleged defect in the application and order is not that they failed to apprise the issuing judge that a cellular tracking device would be used to do real-time tracking that involved initiating a signal, but that they failed to go into greater detail about that technology.[67] However, search warrants need not "include a specification of the precise

---

[66] *See United States v. Karo*, 468 U.S. at 718 (warrant for location tracking will likely satisfy the Fourth Amendment's particularity requirement if law enforcement "describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested"); *see also State v. Tate*, 849 N.W.2d at 810 (particularity requirement was met when an order identified the tracked cell phone by its assigned phone number); *see also United States v. Ringmaiden*, 2013 WL 1932800 at *17 (D. Ariz. 2013) (particularity requirement was met when a warrant identified the aircard to be tracked by description, telephone number, and device serial number).

[67] The Dissenting Opinion argues that the good faith exception cannot be applied in this case because the order was "facially deficient" as a search warrant in that it was "silent" regarding the details of how a cell site simulator works. Dissenting Opinion at 11. However, statutes that implement the requirements of the Fourth Amendment for searches arguably more intrusive than one undertaken with a cell site simulator do not require an officer explain in detail the technical specifications of a particular device used to carry out a proposed search. For example, the statutes governing the authorization of a wiretap – essentially, a search warrant that allows for the interception of private communications in real time – do not require such detail. *See* CJ §10-401 *et seq*. (Maryland wiretap statute); 18 U.S.C. §2510 *et seq.* (federal wiretap statute). (As the excerpts from the Maryland Wiretap Statute quoted in the Dissenting Opinion illustrate, those statutes do not specify the technology used to effect a wiretap other than to refer to it as an "electronic, mechanical or other device." Dissenting Opinion at 13-20). Rather, an application for a wiretap under those statutes describes the probable cause supporting the issuance of the order, the crimes under investigation, the period of the proposed interception, the type of communications sought to be intercepted, the persons likely to be involved in those communications, the efforts to minimize the interception of non-pertinent communications, and related matters. *See* ABA Standards for Criminal Justice – Electronic Surveillance (3d ed. 2001) at 91-166 (detailing standards for wiretap application and order); United States Attorneys' Manual, Criminal Resource Manual, Chapters 28 (Electronic Surveillance – Title III Applications),

manner in which they are to be executed." *Dalia*, 441 U.S. at 257. It is true that the application and the related order suffer from vices endemic to many legal documents – grammatically-challenged prose, repetitive phrasing, multi-paragraph sentences, numerous subordinate clauses, parades of synonyms, legions of commas interspersed with semi-colons. Yet the application and order clearly inform a reasonably diligent reader of what the officers seek to do and how they plan to do it (even if they do not describe the technical details).

The application states that the detectives wished to use, in addition to the pen register and trap and trace device, a "Cellular Tracking Device" and "Real Time Tracking Tool"; among other things, that they would employ "surreptitious or duplication of facilities" and "initiate a signal to determine the location of the subject's mobile phone"; and that they will be engaged in "real time tracking" of a particular cell phone identified by number. A fair reading of this order would encompass a cell site simulator. Certainly, there could have been more detail. Undoubtedly, the application could have been clearer. But that hardly means that the order is "facially invalid" as clearly lacking particularity.

With respect to the nondisclosure agreement discussed in *Andrews*, the testimony at the hearing in *this* case was that the detectives would have answered any questions of the

---

https://www.justice.gov/usam/criminal-resource-manual-28-electronic-surveillance-title-iii-applications [https://perma.cc/6EDW-MPYD], 92 (Title III Procedures – Attachment C – Title III Wire Affidavit Checklist for Law Enforcement Agents), https://www.justice.gov/usam/criminal-resource-manual-92-title-iii-procedures-attachment-c [https://perma.cc/P2ZU-Q84X]. Nor do law enforcement officers typically go beyond the requirements of those statutes to detail the particular technology utilized to effect a wiretap when applying for one. *Id.* Indeed, the Supreme Court has explicitly held that there is no requirement that they do so. *Dalia*, 441 U.S. at 257.

issuing judge about what they planned to do. Even if we ignore that testimony, *Dalia* rejects any requirement that law enforcement officials spell out, in precise detail, their intended method of surveillance when applying for a warrant. This does not mean that the authorizing judge was *required* to sign the order if the detectives had declined to answer questions about the details.[68] But it does mean that the absence of greater detail does not render the order that was issued so fatally deficient that the detectives could not execute it in good faith.

III

Conclusion

For the reasons explained above, we hold that, based on existing case law, it was objectively reasonable for the detectives to believe that their use of the cell site simulator pursuant to the court order was permissible under the Fourth Amendment. Given that the Supreme Court has instructed that suppression should be a "last result" and not a "first impulse," this is an appropriate case for application of the good faith exception. We hold, therefore, that evidence obtained as a result of detectives' use of the cell site simulator should not be suppressed because of use of that device.

JUDGMENT OF THE COURT OF SPECIAL APPEALS REVERSED. COSTS TO BE PAID BY RESPONDENT.

[68] The judge to whom an application is presented can certainly ask for technical information, if the judge believes that it will be helpful to the decision whether to approve the warrant. If the judge does so, the officers may not mislead the judge. But, in the absence of such a request, the failure to provide technical details in an application is not fatal to a warrant.

Circuit Court for Baltimore City
Case No. 114090005
Argued: April 3, 2017

IN THE COURT OF APPEALS

OF MARYLAND

No. 84

September Term, 2016

STATE OF MARYLAND

v.

ROBERT L. COPES, JR.

Barbera, C.J.,
Greene,
Adkins,
McDonald,
Watts,
Hotten,
Getty,

JJ.

Dissenting opinion by Hotten, J., which Greene and Adkins, JJ., join.

Filed: July 28, 2017

Respectfully, I dissent from the majority opinion in this case. I agree with my brethren on the Court of Special Appeals that "… the use of a cell site simulator requires a valid search warrant, or an order satisfying the constitutional requirements of a warrant, unless an established exception to the warrant requirement applies[,]" and that the use of a pen register/trap and trace order to use a cell site simulator in this case was insufficient to satisfy that threshold. *State v. Andrews*, 227 Md. App. 350, 355, 134 A.3d 324, 327 (2016).

For an issuing judge to appreciate the gravity of the exercise of the requirements and parameters of the Fourth Amendment and any intrusion on a person's privacy rights, the issuing judge must appreciate the scope and manner of the search proposed to be conducted. The more an issuing judge understands the technology associated with the device sought to be used, the better the issuing judge can appreciate the constitutional impact of the search request, particularly when the device has the capacity to conduct a very broad, intrusive search impacting the Fourth Amendment. As the Court of Special Appeals eloquently stated, "[t]he analytical framework requires analysis of the functionality of the surveillance device and the range of information potentially revealed by its use." *Andrews*, 227 Md. App. at 376, 134 A.3d at 338.

In the case at bar, the Baltimore City Police Department ("BCPD") relied on Courts & Judicial Proceedings Article ("Cts. & Jud. Proc.") §10-4B-03 as its basis for seeking an order to use the Hailstorm device to locate a cell phone that was associated with the victim, Ina Jenkins. Cts. & Jud. Proc. §10-4B-03 states:

Application or extension of order by investigative or law enforcement officers

(a) An investigative or law enforcement officer may make application for an order or an extension of an order under §10-4B-04 of this subtitle or approving the installation and use of a pen register or a trap and trace device, in writing, under oath or equivalent affirmation, to a court of competent jurisdiction of this State.

Contents of application

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

Cts. & Jud. Proc. §10-4B-01 defines "pen register" and "trap and trace" as follows:

(c) (1) "Pen register" means a device or process that records and decodes dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.

* * *

(d) (1) "Trap and trace device" means a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.

* * *

The cell site simulator (hereinafter "Hailstorm device") used by the BCPD in this case differs from both a pen register and trap & trace because it actively seeks out and provides real time location, and other information, regarding a cell phone and, presumably, the person using it.

Detective John Haley ("Det. Haley"), a member of BCPD's Advanced Technical Team, asserted at the suppression hearing that the Hailstorm device "acts like a cell tower[,]" but then explained that when a police officer inputs the unique electronic serial number ("ESN") associated with a specific cell phone into the Hailstorm device, the device then actively seeks out the location of that cell phone – unlike a cell phone tower, which passively awaits connection to a cell phone. Det. Haley also explained that once the Hailstorm device locates the target cell phone, "the phone thinks that the Hailstorm is the tower, the cell site. So the phone is going to connect with the Hailstorm." Upon connecting to the Hailstorm device, the target cell phone cannot be used, except to call 9-1-1, until the cell phone is disconnected from the Hailstorm device.

Det. Haley acknowledged that, in addition to locating the target cell phone, the Hailstorm device also collects the cell phone information for each cell phone that is located within a two-block radius of the device and is located on the same channel[1] that the Hailstorm device is using.[2] Det. Haley also acknowledged that the Hailstorm device sends a signal that "goes inside" private homes in search of the target cell phone, and that the

[1] Det. Haley explained that Verizon, the service provider in this case, has about ten channels and that cell phones in a given area will seek out the strongest channel to transmit signals. Det. Haley also explained that the Hailstorm device works the same way, it surveys the area where it is activated to determine the strongest channel to transmit, and utilizes that channel to locate the target cell phone. Det. Haley acknowledged that the Hailstorm device can collect the information of anywhere between dozens to hundreds of cell phones that are not the target phone the Hailstorm device is searching for.

[2] Det. Haley testified that at the end of each night the police delete all the cell phone information that was stored on the Hailstorm device from its use during the day.

police did not obtain a separate warrant for 4014 Penhurst Avenue – where the target cell phone in this case was ultimately located. Thus, the Hailstorm device collects far more information than what is authorized by the statutory scope of the Maryland Pen Register statute.

Although the Majority does not hinge its analysis on the question of whether the Pen Register/Trap & Trace and Cellular Tracking Device order relied on in this case was constitutionally sufficient – it assumes that the order was inadequate for the purposes of the opinion – the Majority, nonetheless recognizes the strength of the State's argument regarding that issue. *See* Maj. Slip Op. at 48. The Majority notes that in *Wisconsin v. Tate*, 849 N.W.2d 798 (Wis. 2014), *cert. denied*, 135 S. Ct. 1166 (2015), the Wisconsin Supreme Court considered a case similar to the case at bar, which concluded that an order based on the state's pen register statute was sufficient to constitute a warrant in light of the content of the application and the order itself. *See id.* at 810. Central to the *Tate* Court's holding was its determination that the Wisconsin pen register statute only required a showing that the information sought would be relevant to an ongoing criminal investigation, and the Court determined that the order was sufficiently particular because it identified a particular phone and "permit[ted] a particularized collection of cell site information for only [that] phone." *Id.*

Significantly, both the *Tate* Court and the Majority do not acknowledge that cell site simulators not only "search" for the target cell phone, but also "search" the surrounding area through the emission of a signal. In the present case, the Hailstorm device, which technologically presents significant surveillance capabilities, not only searched for the

target cell phone, but also searched all of the residences in the two block radius of the device, including Respondent's residence at 4014 Penhurst Avenue. This type of search is similar, factually, to the circumstances in *Kyllo v. United States*, 533 U.S. 27, 121 S. Ct. 2038 (2001), where the United States Supreme Court held that the use of thermal energy technology constituted a search for the purposes of the Fourth Amendment, when the police used the technology to detect heat emissions from the defendant's home. *Id.* at 34, 121 S. Ct. at 2043. The Supreme Court concluded in *Kyllo* that "[w]here … the Government uses a device that is not in general public use, to explore the details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* at 40, 121 S. Ct. at 2046. Here, the police utilized the Hailstorm device – technology that was not available to the public – to actively seek out the location of a cell phone through the emission of a signal that "explore[d] the details" of the residences within a two-block radius of the Hailstorm device "that would have previously been unknowable without" the intrusion of the signal. *See id.*

The State concedes for the purposes of this case that the use of the Hailstorm device to locate the target phone constituted a "search" within the meaning of the Fourth Amendment, but argues that the Pen Register/Trap & Trace and Cellular Tracking Device order was constitutionally sufficient to authorize the use of the Hailstorm device to search for the target cell phone, *i.e.* the equivalent of obtaining a search warrant. The pen register order in this case stated that, pursuant to Cts. & Jud. Proc. §10-4B-04: [3]

[3] Cts. & Jud. Proc. §10-4B-04 states, in relevant part:

(continued . . .)

that as part of a criminal investigation of Unknown Person or Persons and others as yet unknown, the Baltimore Police Department (BPD), Drug Enforcement Agency (DEA), Federal Bureau of Investigation (FBI), United States Marshals Service (USMS), United States Secret Service (USSS), Immigration Customs Enforcement (ICE), Alcohol Tobacco and Firearms

---

(. . . continued)

Information obtained relevant to criminal investigations

(a) (1) Upon application made under §10-4B-03 of this subtitle, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation.

* * *

Contents of order

(b) An order issued under this section shall:
(1) Specify the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;
(2) Specify the identity, if known, of the person who is the subject of the criminal investigation;
(3) Specify the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of a trap and trace device, the geographic limits of the trap and trace order;
(4) Contain a description of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and
(5) Direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under §10-4B-05 of this subtitle.

Duration of order

(c) (1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed 60 days.

* * *

(ATF), Sytech, or any other designated law enforcement agency (hereinafter referred to as "Agencies") are authorized to use for a period of sixty (60) days from the date of installation, a Pen Register \ Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits, which shall be installed and used within the jurisdiction of this Court, upon the telephone having the number(s): [XXX-XX] -4686, a AT&T; Sprint/Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider, telephone; and it is further

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

* * *

The Majority notes that the order authorizes the BCPD to use a "Cellular Tracking Device" and "Real Time Tracking Tool" to, among other things, employ "surreptitious or duplication of facilities" and "initiate a signal to determine the location of the subject's mobile phone" and that they will be engaged in "real time tracking" of the specific cell phone identified by number. *See* Maj. Slip Op. at 51. The Majority does not take into account that the terms "Cellular Tracking Device" and "Real Time Tracking Tool" are neither referenced nor defined in the Maryland Pen Register Statute, and that neither the application nor the order in this case provide definitions for those terms. In fact, the pen

register application submitted in this case, and the resulting order, omitted any description of the Hailstorm device. Additionally, the description of the activity that the order authorizes, specifically the authority to "initiate a signal" does not adequately describe how the Hailstorm device works. As noted, *supra*, the Hailstorm device not only emits a signal to locate the target phone, but it also forcibly connects the target cell phone to the device, rendering the phone inoperable by the user for the duration that the phone is connected to the Hailstorm device.

Even ignoring the fact that the order relied on a statute that did not authorize the type of technology that was used, the order also did not comply with the particularity requirement because it failed to adequately describe "the place to be searched[.]" *See United States v. Grubbs*, 547 U.S. 90, 97, 126 S. Ct. 1494, 1500 (2006). While the order did identify the specific cell phone that would be targeted by the Hailstorm device, the order failed to adequately describe "the place to be searched" because it did not state that the Hailstorm device would be used to conduct a search of the Penhurst neighborhood, let alone Respondent's specific residence. Accordingly, to the extent the Majority found the State's argument persuasive that the pen register order in this case was constitutionally sufficient, I respectfully disagree. *See* Maj. Slip Op. at 48.

I also disagree with the Majority's conclusion that the police officers in this case were engaged in "objectively reasonable law enforcement activity" when they used the Hailstorm device in reliance on the language contained in the Pen Register/Trap & Trace and Cellular Tracking Device order. The Majority found persuasive Detective Brian Kershaw's ("Det. Kershaw") testimony that applications for similar orders had been

approved "many, many times" and were never denied. *See* Maj. Slip Op. at 48. The Majority acknowledged that the BCPD was subject to a nondisclosure agreement regarding the Hailstorm technology,[4] but determined that "the testimony at the hearing in *this* case was that the detectives would have answered any questions of the issuing judge about what they planned to do." Maj. Slip Op. at 51-52 (emphasis in original). While it is true that Det. Haley testified that he would have answered any questions that the issuing judge may have had regarding the modified language in the application and order, I find it disingenuous for Det. Haley to state in 2016 that he would have been forthcoming about the Hailstorm technology at the time the order was issued in February 2014, in light of the nondisclosure agreement, which he acknowledged required Baltimore City police officers "to basically not talk about the – not talk about the Hailstorm."

The Supreme Court has held that there are four circumstances where the good faith exception to the exclusionary rule does not apply, and suppression remains the appropriate remedy if: (1) the magistrate or judge issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his or her reckless disregard of the truth; (2) the issuing magistrate has wholly abandoned his or her judicial role; (3) the warrant is based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) the warrant

[4] *See Andrews*, 227 Md. App. at 374-77, 134 A.3d at 337-339 (discussing the terms of the nondisclosure agreement entered into between the State's Attorney for Baltimore City and the Federal Bureau of Investigation as a condition of the Baltimore City Police Department's use of "certain 'wireless collection equipment/technology manufactured by [the] Harris [Corporation].'").

is so facially deficient – *i.e.* failing to particularize the place to be searched or the things to be seized – that the executing officers cannot reasonably presume it to be valid. *See United States v. Leon*, 468 U.S. 897, 923, 104 S. Ct. 3405, 3421 (1984) (citations omitted). The Majority concluded that none of the four reasons identified by the *Leon* Court applied in the present case. I disagree. I find that the fourth circumstance is applicable in this case because it was unreasonable for the police officers to presume that the Pen Register/Trap & Trace and Cellular Tracking Device order was sufficient to authorize their use of the Hailstorm device. As noted, *supra*, the Hailstorm device does not only conduct a Fourth Amendment search for a specific cell phone, it also conducts a Fourth Amendment search of the surrounding area. Accordingly, for the Pen Register/Trap & Trace and Cellular Tracking Device to be facially sufficient to authorize the use of the Hailstorm device it was required to specify the place to be searched, *i.e.* the area where the police officers intended to employ the Hailstorm device. The order does not reference a specific area the police intended to employ the Hailstorm device, it only referenced the cell phone number that was subject to the order.

The order also failed to adequately describe the type of technology that the police officers intended to use in this case. The Majority asserts that the alleged defect in the application and order is not that they failed to apprise the issuing judge that a cellular tracking device would be used to do real-time tracking that involved initiating a signal, but that they failed to go into greater detail about that technology. *See* Maj. Slip Op. at 50. The Majority then concludes that "the application and order clearly inform a reasonably diligent reader of what the officers seek to do and how they plan to do it (even if they do not describe

the details)." *Id.* I disagree. I find that the application and order are silent regarding the Hailstorm technology and how it functions. As noted, *supra*, the Hailstorm device does not just "initiate a signal" to track a cell phone, it forces the target cell phone to connect to the device, rendering the target cell phone inoperable for the duration that it is connected to the Hailstorm device. The Hailstorm device also collects the cell phone information of all surrounding cell phones that are located within a two-block radius of the Hailstorm device and use the same channel that the Hailstorm device utilizes to emit its signal. Nothing in the language of the application or order in this case suggests that the police intended to use this type of invasive technology.

The Majority observes in a footnote that "statutes that implement the requirements of the Fourth Amendment for searches arguably more intrusive than one undertaken with a cell site simulator do not require an officer [to] explain in detail the technical specifications of a particular device used to carry out a proposed search." Maj. Slip Op. at 50 n. 67. As an example, the Majority notes that "the statutes governing the authorization of a wiretap – essentially, a search warrant that allows for the interception of private communications in real time – do not require such [technical] detail." *Id.* (citing Cts. & Jud. Proc. §10-401, *et seq.*; 18 U.S.C. §2510, *et seq.*). The Majority summarizes the requirements necessary for an application to obtain a wiretap pursuant to the above-referenced statutes, and concludes that police officers neither "go beyond the requirements of those statutes to detail the particular technology utilized to effect a wiretap when applying for one[,]" nor are required to do so, pursuant to the U.S. Supreme Court decision in *Dalia v. United* States, 441 U.S. 238, 99 S. Ct. 1682 (1979), which explicitly held there

was no requirement that they do so. *See id.* (citing *Dalia*, 441 U.S. at 257, 99 S. Ct. at 1693).

In relying on the wiretapping statutes in support of its view, the Majority does not consider the fact that, unlike the procedures set forth in the wiretapping statutes, at all times relevant to this case, there was no statute governing the use of cell site simulators. *Cf.* Criminal Procedure Article §1-203.1 (effective October 1, 2014). Additionally, while it is true that the wiretapping statutes, and other statutes implementing the requirements of the Fourth Amendment for searches, do not require a detailed recitation of the technical specifications of a particular device an officer plans to use, no such detail is required precisely because there is a statute that governs the use of the technology and describes the technology that is intended to be used to conduct the Fourth Amendment search. Considering the Majority's example of the Maryland wiretapping statute, Cts. & Jud. Proc. §10-406(a) states that:

> (a) The Attorney General, State Prosecutor, or any State's Attorney may apply to a judge of competent jurisdiction, and the judge, in accordance with the provisions of §10-408 of this subtitle, may grant an order authorizing the interception of wire, oral, or electronic communications by investigative or law enforcement officers when the interception may provide or has provided evidence of the commission of:
> (1) Murder;
> (2) Kidnapping;
> (3) Rape;
> (4) A sexual offense in the first or second degree;
> (5) Child abuse in the first or second degree;
> (6) Child pornography under §11-207, §11-208, or §11-208.1 of the Criminal Law Article;
> (7) Gambling;
> (8) Robbery under §3-402 or §3-403 of the Criminal Law Article;

(9) A felony under Title 6, Subtitle 1 of the Criminal Law Article;
(10) Bribery;
(11) Extortion;
(12) Dealing in a controlled dangerous substance, including a violation of §5-617 or §5-619 of the Criminal Law Article;
(13) A fraudulent insurance act, as defined in Title 27, Subtitle 4 of the Insurance Article;
(14) An offense relating to destructive devices under §4-503 of the Criminal Law Article;
(15) A human trafficking offense under §11-303 of the Criminal Law Article;
(16) Sexual solicitation of a minor under §3-324 of the Criminal Law Article;
(17) An offense relating to obstructing justice under §9-302, §9-303, or §9-305 of the Criminal Law Article;
(18) Sexual abuse of a minor under §3-602 of the Criminal Law Article;
(19) A theft scheme or continuing course of conduct under §7-103(f) of the Criminal Law Article involving an aggregate value of property or sources or services of at least $10,000;
(20) Abuse or neglect of a vulnerable adult under §3-604 or §3-605 of the Criminal Law Article;
(21) An offense relating to Medicaid fraud under §§8-509 through §8-515 of the Criminal Law Article; or
(22) A conspiracy or solicitation to commit an offense listed in items (1) through (21) of this subsection.

Cts. & Jud. Proc. §10-408 states, in relevant part:

Applications for interception in writing

(a) (1) Each application for an order authorizing the interception of a wire, oral, or electronic communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make the application. Each application shall include the following information:
(i) The identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(ii) A full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including:
1. Details as to the particular offense that has been, is being, or is about to be committed;
2. Except as provided in paragraph (2) of this subsection, a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted;
3. A particular description of the type of communications sought to be intercepted; and
4. The identity of the person, if known, committing the offense and whose communications are to be intercepted;

(iii) A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(iv) A statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe additional communications of the same type will occur thereafter;

(v) A full and complete statement of the facts concerning all previous applications known to the individual authoring and making application, made to any judge for authorization to intercept wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each application; and

(vi) Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain the results.

(2) (i) In the case of an application authorizing the interception of an oral communication, a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted is not required if the application:
1. Is by an investigative or law enforcement officer;
2. Is approved by the Attorney General, the State Prosecutor, or a State's Attorney;
3. Contains a full and complete statement as to why specification of the nature and location of the facilities from

which or the place where the communication is to be intercepted is not practical; and

4. Identifies the individual committing the offense and whose communications are to be intercepted.

(ii) In the case of an application authorizing the interception of a wire or electronic communication, a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted is not required if the application:

1. Is by an investigative or law enforcement officer;
2. Is approved by the Attorney General, the State Prosecutor, or a State's Attorney;
3. Identifies the individual believed to be committing the offense and whose communications are to be intercepted;
4. Makes a showing that there is probable cause to believe that the individual's actions could have the effect of thwarting interception from a specified facility; and
5. Specifies that interception will be limited to any period of time when the investigative or law enforcement officer has a reasonable, articulable belief that the individual identified in the application will be proximate to the communication device and will be using the communication device through which the communication will be transmitted.

* * *

Grounds for ex parte interception order

(c) (1) Upon the application the judge may enter an ex parte order, as requested or as modified, authorizing interception of wire, oral, or electronic communications within the territorial jurisdiction permitted under paragraphs (2) and (3) of this subsection, if the judge determines on the basis of the facts submitted by the applicant that:

(i) There is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in §10-406 of this subtitle;

(ii) There is probable cause for belief that particular communications concerning that offense will be obtained through interception;

(iii) Normal investigative procedures have been tried and have failed or reasonable appear to be unlikely to succeed if tried or to be too dangerous; and

(iv) There is probable cause for belief:

1. That the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of the offense, or are leased to, listed in the name of, or commonly used by this person in accordance with subsection (a)(1) of this section; or
2. That the actions of the individual whose communications are to be intercepted could have the effect of thwarting an interception from a specified facility in accordance with subsection (a)(2) of this section.

(2) Except as provided in paragraphs (3) and (4) of this subsection, an ex parte order issued under paragraph (1) of this subsection may authorize the interception of wire, oral, or electronic communications only within the territorial jurisdiction of the court in which the application was filed.

(3) If an application for an ex parte order is made by the Attorney General, the State Prosecutor, or a State's Attorney, an order issued under paragraph (1) of this subsection may authorize the interception of communications received or sent by a communication device anywhere within the State so as to permit the interception of the communications regardless of whether the communication device is physically located within the jurisdiction of the court in which the application was filed at the time of the interception. The application must allege that the offense being investigated may transpire in the jurisdiction of the court in which the application is filed.

(4) In accordance with this subsection, a judge of competent jurisdiction may authorize continued interception within the State, both within and outside the judge's jurisdiction, if the original interception occurred within the judge's jurisdiction.

Contents of ex parte interception orders

(d) (1) Each order authorizing the interception of any wire, oral, or electronic communication shall specify:

(i) The identity of the person, if known or required under subsection (a)(2) of this section, whose communications are to be intercepted;

(ii) The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted, if known;

(iii) A particular description of the type of communications sought to be intercepted, and a statement of the particular offense to which it relates;

(iv) The identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(v) The period of time during which the interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

(2) An order authorizing the interception of a wire, oral, or electronic communication, upon request of the applicant, shall direct that a provider of wire or electronic communication service, landlord, custodian or other person furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that the service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing the facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing facilities or assistance.

* * *

Motions to suppress by aggrieved persons

(i) (1) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of this State or a political subdivision thereof, may move to suppress the contents of any intercepted wire, oral, or electronic communication, or evidence derived therefrom, on the grounds that:

(i) The communication was unlawfully intercepted;

(ii) The order of authorization under which it was intercepted is insufficient on its face, or was not obtained or issued in strict compliance with this subtitle; or

(iii) The interception was not made in conformity with the order of authorization.

* * *

Cts. & Jud. Proc. §10-401(10) defines "[i]ntercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communications through the use of any

electronic, mechanical, or other device." Cts. & Jud. Proc. §10-401(5)(i) defines "[e]lectronic communication" as "any transfer of signs, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." Sub-paragraph (ii) also states that "electronic communication does not include: (1) [a]ny wire or oral communication; (2) [a]ny communication made through a tone-only paging device; or (3) [a]ny communication from a tracking device." An "[o]ral communication" is defined to mean "any conversation or words spoken to or by any person in a private conversation." Cts. & Jud. Proc. §10-401(13)(i). The statutes also defines "[w]ire communication" as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of a connection in a switching station) furnished or operated by any person licensed to engage in providing or operating such facilities for the transmission of communications.

Cts. & Jud. Proc. §10-401(18). Finally, Cts. & Jud. Proc. §10-401(8) defines "[e]lectronic, mechanical, or other device" to mean

> any device or electronic communication other than:
>
> (i) Any telephone or telegraph instrument, equipment or other facility for the transmission of electronic communications or any component thereof,
>
> (a) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by the subscriber or user for connection to the facilities of the service and used in the ordinary course of its business; or

(b) being used by a communications common carrier[5] in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; or

(ii) A hearing aid or similar device being used to correct subnormal hearing to not better than normal.

As noted, *supra*, and in contrast to the above-quoted statutory scheme for wiretapping in the State of Maryland, the order relied on by the police in the present case was based on the Maryland Pen Register Statute, which exclusively describes the pen register and trap & trace technologies and neither of which remotely describe cell site simulator technology. *See* Cts. & Jud. Proc. §10-4B-01(c)(1), (d)(1). Thus, while as a general matter it is true that when a law enforcement officer is applying for a search warrant pursuant to a statute that "implement[s] the requirements of the Fourth Amendment for searches" he or she is not required to "go beyond the requirements of those statutes to detail the particular technology utilized." *See* Maj. Slip Op. at 50 n. 67; *see also Dalia*, 441 U.S. at 257, 99 S. Ct. at 1693. Where, as in this case, however, a law enforcement officer does not rely on a statute that details the type of technology the warrant, or order in this case, would apply to, he or she is required to provide a description of the technology he or she intends to use in sufficient detail for an issuing judge to appreciate the scope of the potential infringement on a person's Fourth Amendment privacy interests, and the officer's failure to do so results in a warrant so deficient on its face that the good faith exception to the exclusionary rule should not apply.

---

[5] The statute defines a "[c]ommunications common carrier" as "any person engaged as a common carrier for hire in the transmission of wire or electronic communications." Cts. & Jud. Proc. §10-401(3).

Accordingly, I conclude it was unreasonable for the police officers in this case to presume that the Pen Register/Trap & Trace and Cellular Tracking Device order authorized them to use the Hailstorm device. The circuit court correctly suppressed the evidence that was subsequently discovered in the Respondent's home.

Judges Greene and Adkins have authorized me to state that they join in this opinion.