Journal of Business & Technology Law

Volume 14 | Issue 1 Article 7

State v. Copes: Surveillance Technology and the Limits of the Good Faith Exception to Fourth Amendment Violations

Elise Desiderio

State v. Copes: Surveillance Technology and the Limits of the Good Faith Exception to Fourth Amendment Violations

ELISE DESIDERIO*

INTRODUCTION

In recent decades, law enforcement officers' ability to surveil citizens has greatly expanded. Audio recording,[1] thermal imaging,[2] and tracking devices[3] allow law enforcement nearly unfettered access to individuals' information, including real-time locations. These technologies can develop at a faster rate than the law adapts to them. Thus, the Fourth Amendment implications of some of these technologies is an

* Elise Desiderio is a Juris Doctor candidate at the University of Maryland Francis King Carey School of Law, Class of 2019, and the Editor-in-Chief of Volume 14 of the *Journal of Business and Technology Law*. She thanks the *Journal* Executive Board and editorial staff for their hard work and support, Professor Rena Steinzor for her invaluable and unwavering mentorship and Professor Danielle Citron for sharing her passion for and deep understanding of privacy law. Most importantly, Elise thanks her family for their love and trust.

[1] Katz v. United States, 389 U.S. 347, 349 (1967) (evaluating police use of a recording device placed on top of a phone booth).

[2] Kyllo v. United States, 533 U.S. 27, 33 (2001) (holding that warrantless use of a thermal imaging device to observe details of a person's home violated the Fourth Amendment).

[3] State v. Copes, 165 A.3d 418, 447 (Md. 2017) (holding that use of a cell site simulator to reveal and track the location of a cell phone is protected by the good faith exception to the Fourth Amendment's exclusionary rule).

open question.[4]

Present issues implicate law enforcement's use of cell site location information (CSLI) and cell site simulators. CSLI provides the historical data available from third-party owned and maintained cell towers so law enforcement may narrow their search area to phones pinging off of those towers.[5] Cell site simulators allow law enforcement to mimic cell towers to capture and track the precise, real-time location of a specific phone.[6] The use of cell site simulators is controversial, particularly in Baltimore City, Maryland, where police have used such devices 4,300 times between 2007 and 2015.[7]

In July 2017, the Maryland Court of Appeals held in *State v. Copes*[8] that while police's warrantless use of a Hailstorm cell site simulator[9] to locate a defendant's cell phone may have violated the Fourth Amendment, an

---

[4] *See Copes*, 165 A.3d at 435 ("Appellate courts have reached different conclusions as to whether the warrantless collection of historical CSLI implicates the Fourth Amendment.").

[5] Carpenter v. United States, 585 U.S. —, slip op. at 11 (2018) (holding that law enforcement must generally acquire a warrant to access CSLI data).

[6] Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, THE BALTIMORE SUN (Apr. 9, 2015), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.

[7] *Id.*

[8] *Copes*, 165 A.3d at 447 (holding that use of a cell site simulator to reveal and track the location of a cell phone is protected by the good faith exception to the Fourth Amendment's exclusionary rule).

[9] "Although 'Stingray' has become a catch-all name for devices of [this] kind, often referred to as 'IMSI catchers,'" Harris Corporation—the company that manufactures and sells most of these devices—sells other "surveillance boxes, including the Hailstorm [at issue in *Copes*], ArrowHead, AmberJack, and KingFish." Sam Biddle, *Long-Secret Stingray Manuals Detail How Police Can Spy on Phones*, THE INTERCEPT, Sep. 12, 2016, https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/.

exception for reasonable law enforcement actions applies to that violation.[10] Generally, courts exclude information obtained in violation of the Fourth Amendment from later use as evidence against the accused in the prosecution's case-in-chief.[11] However, the Supreme Court determined that an exception to this exclusionary rule applies where law enforcement acted reasonably, or in good faith, including when police reasonably rely on a warrant that is later determined to be invalid.[12]

The Court of Appeals' reasoning in *Copes* is flawed for three reasons. First, the court declined to make a definitive finding that law enforcement violated Copes' Fourth Amendment rights.[13] Second, the court expanded its construction of the good faith exception when it found that the law enforcement officers acted in good faith in using the cell site simulator.[14] Finally, the court declined to follow soundly reasoned precedent set forth in *State v. Andrews*, a Maryland Court of Special Appeals case largely in synthesis

---

[10] Instead of defining "search" by its plain meaning (to seek out or to find), the Supreme Court defines a "search" as a violation of a "subjective manifestation of privacy" that "society is willing to accept as reasonable." Katz v. United States, 389 U.S. 347, 361 (1967) (J. Harlan, concurring). This definition, decided upon after increasingly prevalent use of surveillance technologies like voice recorders, has made the job of pinning down what a search is under the Fourth Amendment more difficult. *See generally Id.* at 347.

[11] *See* Herring v. United States, 555 U.S. 135, 139–140 (2009) (opining that the exclusionary rule is a judicially created doctrine that allows courts to exclude evidence obtained through some, but not all, Fourth Amendment violations).

[12] United States v. Leon, 468 U.S. 897, 918–919 (1984) (establishing the good faith exception by holding that, where police officers acted reasonably based on a mistakenly issued warrant, the exclusionary rule should not apply because enforcement of the rule would have no deterrent effect against future bad acts by law enforcement).

[13] *See infra* Part II.A.; *Copes*, 165 A.3d at 431.

[14] *See infra* Part II.B.; *Copes*, 165 A.3d at 444.

with *Copes*.[15] In *Andrews*, the court held that warrantless use of cell site simulators is generally impermissible.[16] The flawed reasoning in *Copes* resulted in a holding that applied the good faith exception to the Fourth Amendment's exclusionary rule too broadly, allowing for unreasonable law enforcement activity while also failing to vindicate accused persons' privacy rights.

I. THE CASE

Robert Copes was charged with murder.[17] At trial, Copes filed a motion to suppress evidence police uncovered using a cell site simulator to locate a phone that officers ultimately learned belonged to him.[18] The police department and the company that sells the Hailstorm cell site simulator police used to locate the phone had entered into a nondisclosure agreement, barring the police department from disclosing its use of the Hailstorm.[19] The non-disclosure agreement also covered officers' pen register applications to magistrates.[20]

---

[15] *Copes*, 165 A.3d at 439 (citing State v. Andrews, 134 A.3d 324 (Md. App. 2016)) (affirming a prior decision to suppress evidence gained using a cell cite simulator; holding that warrantless use of cell site simulators is generally impermissible).

[16] *See infra* Part II.C.; State v. Andrews, 134 A.3d 324 (Md. App. 2016).

[17] *Copes*, 165 A.3d at 429.

[18] *Id.*

[19] *Id.*; *see also* Fenton, *supra* note 6.

[20] "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. . . [.] 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 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." *Copes*, 165 A.3d at 424 (citing Smith v. Maryland, 442 U.S. 735 (1979)); *see also* Pen Register Statute, MD. CODE ANN., CTS. & JUD. PRO. § 10–4B–01(c)(1) ("'Pen register' means a device

The trial court granted Copes' motion to suppress.[21] The state of Maryland appealed the circuit court's decision, and the Court of Special Appeals affirmed.[22] The Court of Appeals granted certiorari.[23]

The Court of Appeals reversed the Court of Special Appeals' decision on three bases. First, the Court of Appeals noted that the Fourth Amendment's exclusionary rule is applicable only when the deterrent effect of applying the rule is substantial and outweighs any negative effect to the justice system.[24] Paramount among these negative effects is the notion that "some guilty defendants may go free or receive reduced sentences . . . offend[ing] basic concepts of the criminal justice system."[25] The exclusionary rule is a judicially created doctrine that allows courts to exclude evidence obtained through some, but not all, Fourth Amendment violations.[26] The rule is "designed to safeguard Fourth Amendment rights generally through its deterrent effect."[27] When evaluating deterrence, "[i]f . . . the exclusionary rule does not result in appreciable deterrence, then, clearly, its use . . . is unwarranted."[28]

Second, the Court of Appeals maintained that "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

---

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.").

[21] *Copes*, 165 A.3d at 430.

[22] *Id.* at 430–431.

[23] *Id.* at 431.

[24] *Id.* at 432 (citing Herring v. United States, 555 U.S. 135, 147 (2009)).

[25] United States v. Leon, 468 U.S. 897, 907–08 (1984).

[26] *Herring*, 555 U.S. at 139–40.

[27] *Id.* (quoting United States v. Calandra, 414 U.S. 338, 348 (1974)).

[28] United States v. Janis, 428 U.S. 433, 454 (1976).

of the Fourth Amendment."[29] Under the facts in *Copes*, the good faith exception's application is based on "objectively reasonable reliance" on a warrant that is found to lack probable cause.[30] The *Copes* court found that, although the use of the Hailstorm was likely a Fourth Amendment search conducted without a warrant,[31] the officers' behavior in using a cell site simulator under a pen register order was objectively reasonable.[32] Accordingly, the Court of Appeals reversed the Court of Special Appeals' decision granting Copes' motion to suppress.[33]

Finally, the *Copes* court found that the pen register order the police acquired was functionally the same as a warrant for Fourth Amendment purposes.[34] The Fourth Amendment's bar against unreasonable searches is "generally satisfied when law enforcement officers obtain a warrant authorizing the search in question."[35] The *Copes* court found that a pen register order was functionally the same as a warrant in part because similar orders, under which police officers used cell site simulators in a similar way, were approved at least semi-regularly.[36] Because the officers relied on a mechanism police regularly used before, the Court of Appeals found that using a pen register for cell site simulators represents objectively reasonable police activity such that the good faith exception should apply.[37]

---

[29] *Copes*, 165 A.3d at 432 (quoting *Leon*, 468 U.S. at 919) (establishing a good faith exception to the exclusionary rule)).
[30] *Herring*, 555 U.S. at 142 (citing *Leon*, 468 U.S. at 922).
[31] *Copes*, 165 A.3d at 431.
[32] *Id.* at 447.
[33] *Id.*
[34] *Id.* at 444.
[35] *Id.* at 440 (citing Riley v. California, — U.S. —, 134 S. Ct. 2473, 2482 (2014)).
[36] *Copes*, 165 A.3d at 444.
[37] *Id.*

In her dissent, Judge Hotten, joined by Judges Greene and Adkins, argued two points: (1) the pen register order was not a search warrant or its functional equivalent;[38] and (2) the good faith exception cannot apply under *United States v. Leon*.[39] First, the dissent noted that a "Hailstorm device collects far more information than what is authorized by the statutory scope of the Maryland Pen Register statute."[40] The Hailstorm device scans not only for the target cell phone, but also the whole two-block radius surrounding the device.[41] This capability, the dissent posited, is like the thermal imaging technology used in *Kyllo*, for which the Supreme Court held law enforcement needed to first acquire a warrant before using.[42]

Second, the dissent found it "unreasonable for the police officers to presume that the Pen Register/Trap [and] Trace and Cellular Tracking Device order was sufficient to authorize their use of the Hailstorm device."[43] The dissent found that the pen register order "was neither represented as a warrant when presented to the issuing judge nor did it comport with the dictates of the Fourth Amendment requiring that a warrant particularly describe the place to be

---

[38] *Id.* at 447.

[39] *Id.*; United States v. Leon, 468 U.S. 897, 923 (1983) (outlining four situations in which the good faith exception is inapplicable: where (1) "the magistrate . . . in issuing a warrant was misled by information in the affidavit that the affiant knew was false or would have known was false, except for his reckless disregard for the truth[;]" (2) the "magistrate wholly abandoned his judicial role[;]" (3) the affidavit is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable[;]" or (4) the warrant is "so facially deficient[, . . .] 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.") (internal quotations and citations omitted).

[40] *Copes*, 165 A.3d at 449.

[41] *Id.*

[42] *Id.*

[43] *Id.* at 452.

[searched or the technology to be used in conducting the search."[44] The dissent's reasoning and conclusions are sound; the following analysis expands upon that reasoning to further address the flaws in the *Copes* majority's holding.

II. ANALYSIS

While the *Copes* majority found that police use of a Hailstorm cell site simulator was likely a warrantless search under the Fourth Amendment,[45] the court declined to make a definitive finding that the officers infringed upon Copes' guaranteed freedom from unreasonable searches, muddying the waters for future defendants. Additionally, the Court of Appeals' decision improperly expanded the good faith exception to the exclusionary rule. In finding that (1) a pen register order is likely functionally the same as a warrant,[46] and (2) disclosure of technological details is not necessary to obtain a valid pen register,[47] the *Copes* court applied the good faith exception too broadly, such that the exception threatens to eclipse the rule. Finally, the *Copes* court failed to vindicate accused persons' Fourth Amendment rights when it declined to follow *State v. Andrews*,[48] a case in synthesis with *Copes*, where the Court of Special Appeals held that the good faith exception is generally inapplicable to warrantless use of cell site simulators.[49]

---

[44] *Id.*
[45] *Copes*, 165 A.3d at 431.
[46] *Id.* at 444.
[47] *Id.* at 446.
[48] State v. Andrews, 134 A.3d 324 (Md. App. 2016) (affirming a prior decision to suppress evidence gained using a cell cite simulator without a search warrant). *Andrews* is a Court of Special Appeals case and is thus not binding on the Court of Appeals. However, the Court of Special Appeals' holding in *Andrews* is well-reasoned and thus represents sound persuasive authority.
[49] *Copes*, 165 A.3d at 447.

A. Use of a cell site simulator to locate and track Copes' phone constitutes a definitive Fourth Amendment violation

The *Copes* court found that police likely engaged in a warrantless search when they used a Hailstorm device to locate his phone and, by extension, Copes himself.[50] However, the court ultimately declined to decide the Fourth Amendment question because the United States Supreme Court granted certiorari to hear *United States v. Carpenter*, a case involving warrantless use of CSLI, not cell site simulators.[51] Articulating its reasoning and referencing *Carpenter*, the Court of Appeals opined: "The Supreme Court has reached varying conclusions about the application of [the

[50] *Id.* at 431.

[51] *Id.* at 447; Carpenter v. United States, 585 U.S. — (2018). Justice Roberts, writing for the majority, recognized the scope of information available to law enforcement from third-party service providers, and indeed "the progress of science[,] has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers [of the United States Constitution], after consulting the lessons of history, drafted the Fourth Amendment to prevent." *Carpenter*, 585 U.S. —, slip op. at 22.

principles laid out in *Katz*[52] and *Kyllo*[53]] to the use of location tracking devices, and has recently agreed to consider such an issue related to cell phones."[54]

The Court of Appeals' reasoning in its decision to defer addressing the Fourth Amendment question is flawed for two reasons. First, the technology at issue in *Carpenter* does not yield results as precise as that used in *Copes*, rendering the Fourth Amendment implications of those technologies not comparable.[55] Second, even considering Supreme Court precedent pre-*Carpenter*, the Court of Appeals should have found that warrantless use of cell site simulators definitively violated the Fourth Amendment, irrespective of the Supreme Court's then-pending decision in *Carpenter*.[56] The *Copes* holding may create instability for future defendants about the suppression of evidence. Such instability then results in a strategic disadvantage to defendants as they move through the criminal justice system.

---

[52] In *Katz v. United States*, the Supreme Court held that the Fourth Amendment protects people, not places. Katz v. United States, 389 U.S. 347, 351 (1967). The *Katz* Court held that Federal Bureau of Investigation officials violated a defendant's Fourth Amendment right against unreasonable search when they placed a listening device on top of a public telephone booth to record a defendant's end of a phone conversation. *Id.* at 354. Though a phone booth is not a constitutionally protected place, because the defendant entered the booth and closed the door before speaking on the phone, the Court found that recording the defendant's end of the conversation from atop the booth was a violation of his Fourth Amendment protections. *Id.* Society is willing to accept that when a person enters a phone booth and closes the door, that person reasonably expects further conversation inside the booth to be private. *Id.* at 359.

[53] *Kyllo*, 533 U.S. at 33 (holding that warrantless use of surveillance technology violates the Fourth Amendment if law enforcement (1) uses technology not in public use (2) to observe details of a private home (3) in a way that would be otherwise impossible without physical intrusion).

[54] *Copes*, 165 A.3d at 433–434.

[55] *See infra* Part II.A.i.

[56] *See infra* Part II.A.ii.

1. The Court of Appeals' decision conflated CSLI and cell site simulators

At issue in *Carpenter* was law enforcement's warrantless acquisition of cell site location information (CSLI).[57] The *Copes* court noted that other courts held that accessing CSLI data was not a Fourth Amendment search.[58] The court also noted that many courts considering CSLI cases cited the "third party doctrine,"[59] which the Supreme Court established when it concluded 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[60] or obtain a depositor's bank records[61] from a financial institution."[62] Finding general points of synthesis between CSLI usage and reliance on pen registers, the *Copes* court declined to decide whether a Fourth Amendment violation occurred when officers used a cell site simulator while executing a pen register order.[63]

---

[57] Carpenter v. United States, 585 U.S. ——, slip op. at 11 (2018) (holding that warrantless acquisition of CSLI does not fall under the good faith exception to the Fourth Amendment's exclusionary rule).
[58] *Copes*, 165 A.3d at 435.
[59] *Id.* at 436; United States v. Graham, 824 F.3d 421, 427–28 (2016) (*en banc*) (holding that a person does not have a reasonable expectation of privacy regarding her cell phone's CSLI because a cell phone user voluntarily shares that information with her service provider whenever she uses the phone to call or text), *abrogated by* Carpenter v. United States, 585 U.S. — (2018).
[60] *See generally* Smith v. Maryland, 442 U.S. 735 (1979) (holding that use of a pen register is not a search under the Fourth Amendment because individuals share the numbers they dial with their service providers).
[61] *See generally* United States v. Miller, 425 U.S. 435 (1976) (holding that obtaining a depositor's bank records is not a search because the depositor shares those records with the bank).
[62] *Copes*, 165 A.3d at 435.
[63] *Id.* at 439.

However, in *Carpenter*, the Court held that "a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party,"[64] and further found that suspects have legitimate privacy interests in their CSLI records because those records are part of an individual's "papers" or "effects."[65]

Even if the third-party doctrine covered CSLI data, CSLI and cell site simulators are not the same or comparable mechanisms, nor do they provide the same or comparable information.[66] Cell site simulators allow for more precise location targeting than CSLI and allow law enforcement to acquire data on their own, without relying on a third party.[67] CSLI provides data available from a third-party cell tower so law enforcement may narrow their search area.[68] Conversely, a cell site simulator allows law enforcement to simulate a cell tower and capture and track the precise location of a specific phone.[69] Because of their nature, capabilities, and invasiveness, cell site simulators are not equivalent to CSLI, and thus neither are their Fourth Amendment implications.

---

[64] *Carpenter*, 585 U.S. ——, slip op. at 21.
[65] *Id.*; U.S. CONST. amend. IV.
[66] When the Sixth Circuit decided *Carpenter*, the court noted "the distinction between GPS tracking and CSLI acquisition," writing that "CSLI does appear to provide significantly less precise information about a person's whereabouts than GPS and, consequently, [the court agrees] that a person's privacy interest in the CSLI his or her cell phone generates may indeed be lesser." United States v. Carpenter, 819 F.3d 880, 894 (6th Cir. 2016), *rev'd by* Carpenter v. United States, 585 U.S. — (2018) (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("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.")).
[67] *See infra* note 84.
[68] *Carpenter*, 585 U.S. —, slip op. at 2 (2018).
[69] *See* Fenton, *supra* note 6.

2. Supreme Court precedent supports a definitive finding that warrantless use of cell site simulators violates individuals' Fourth Amendment protection against unreasonable searches

Supreme Court precedent, set in *Kyllo v. United States*, supports a holding that the warrantless use of surveillance technology violates the Fourth Amendment when law enforcement (1) uses technology not in public use; (2) to observe details of a private home; (3) in a way that would be otherwise impossible without physical intrusion.[70] Use of the cell site simulator, at issue in *Copes*, satisfies all three factors required under *Kyllo*.[71]

First, the officers relied on a surveillance method not in public use.[72] Cell site simulators sold by Harris Corporation are only available to police departments and federal agencies; systems may cost $27,800, excluding software and accessories.[73] Second, the officers observed details of a private home, namely Copes' real-time location within his apartment.[74] Finally, the officers observed those details in a manner that would have been otherwise impossible without physical intrusion.[75] The officers could not have located the defendant within the building without physical intrusion of that building.[76] Instead of physically intruding, the officers located the building by intercepting a

[70] *Kyllo*, 533 U.S. at 33.
[71] *Id.*
[72] *Id.*
[73] Curtis Waltman, *Here's How Much a StingRay Cell Phone Surveillance Tool Costs*, VICE: MOTHERBOARD (Dec. 8, 2016), https://motherboard.vice.com/en_us/article/gv5k3x/heres-how-much-a-stingray-cell-phone-surveillance-tool-costs.
[74] *Copes*, 165 A.3d at 421.
[75] *Id.*
[76] *Id.*

cell phone signal to find the phone's precise location inside the building.[77] Thus, warrantless use of a cell site simulator to precisely locate Copes' phone—and, by extension, Copes himself—violated Copes' Fourth Amendment protections under *Kyllo*.[78]

B. The Court of Appeals erroneously applied the good faith exception

The *Copes* court found that it was not clear to the detectives that the use of a pen register to employ a cell site simulator failed to satisfy the Fourth Amendment's warrant requirement.[79] In so finding, the Court of Appeals relied on testimony from "Detective Kershaw, [who stated that] applications for similar orders had been approved 'many, many times,' and never denied."[80] Because of law enforcement's prior reliance on these pen register orders, the *Copes* court found that law enforcement acted reasonably.[81] The court found that the officers' actions were reasonable independent of whether (1) pen register orders were a valid basis on which to surveil using a Hailstorm device; and (2) the magistrate approving the order was aware that police planned to use a Hailstorm device.[82]

The Supreme Court in *United States v. Leon* described four situations in which the good faith exception to the exclusionary rule does *not* apply.[83] These situations are as follows:

---

[77] *Id.*
[78] *Kyllo*, 533 U.S. at 33.
[79] *Copes*, 165 A.3d at 444.
[80] *Id.*
[81] *Id.* at 447.
[82] *Id.* at 444, 446.
[83] *Leon*, 468 U.S. at 923.

> (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 [as] to render official belief in its 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.[84]

First, a pen register order is not comparable to a warrant in form or function.[85] The good faith exception, as applied to the facts in *Copes*, requires officers' reasonable reliance on an invalid warrant or what the officers reasonably believed to be its functional equivalent;[86] therefore, the good faith exception should not apply to officers' reliance on a pen register order in *Copes*. Second, even if the pen register order were considered functionally equivalent to a warrant, the facts in *Copes* speak to the first situation under *Leon*, rendering the good faith exception inapplicable for misleading an issuing magistrate, by omitting the planned use of a cell site simulator.[87]

---

[84] *Copes*, 165 A.3d at 433 (citing *Leon*, 468 U.S. at 923).
[85] *See infra* Part II.B.i.
[86] *Id.*
[87] *See infra* Part II.B.ii.

1. The good faith exception requires reasonable reliance on a warrant that is later found invalid; pen register orders are not functionally equivalent to warrants

A pen register order is not a warrant,[88] nor is a pen register order functionally the same as a warrant.[89] A pen register "records the numbers dialed out from a given phone," while related technology known as a "trap and trace device records the numbers that dial into that phone."[90] Importantly, a pen register order is easier for law enforcement to acquire than a search warrant. An application for a pen register order requires:

---

[88] Use of a pen register alone is not a "search" under the Fourth Amendment, as the Supreme Court noted in *Smith v. Maryland*. Smith v. Maryland, 442 U.S. 735, 745–746 (1979). However, contemporary technology allows for the gathering of far more information, in real-time, than the phone numbers dialed out that officers acquired in *Smith*. *Id.*; Carpenter v. United States, 585 U.S. —, slip op. at 11 (declining to extend *Smith* to include CLSI). Moreover, precedent suggests that pen register orders have limits. The Supreme Court in *Riley v. California* "reject[ed] the . . . suggesting that officers should always be able to search a phone's call log." *Riley*, 134 S. Ct. 2473, 2492 (2014) (holding that officers could not go through the call logs of a suspect's cell phone without a warrant). A pen register may have, in its earlier uses, been a way to access call logs, as in *Smith*, but in *Copes*, officers used the same type of order to not only record phone numbers dialed in and out from a cell phone, but the real-time, "fairly accurate estimate of the target phone's location." *Copes*, 165 A.3d at 423. *See also Copes*, 165 A.3d at 423 n.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.").

[89] *Copes*, 165 A.3d at 440.

[90] *Id.* at 424.

> (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.[91]

A search warrant application, in contrast, requires law enforcement to provide a sworn affidavit stating that "there is probable cause to believe" either a crime is being committed within the issuing judge's jurisdiction or "property subject to seizure under the criminal laws of the State is on the person or in or on the building apartment, premises, place, or thing."[92] Because a pen register application is less stringent than a search warrant petition, officers need not be as certain about the nature or specificity of the information they anticipate uncovering through surveillance executed under a pen register.[93]

The District of Columbia Court of Appeals recently considered the question of whether the good faith exception applies when officers use a cell site simulator without a warrant, and held that the good faith exception is inapplicable in such cases.[94] *Jones v. United States*, decided September 21, 2017, is a crucial holding from an influential court rejecting application of a good faith exception in warrantless cell site simulator cases.[95] The *Jones* court rejected assertions that the *Copes* court accepted, namely that (1) "at the time of [the] incident, no court had held that

---

[91] MD. CODE ANN., CTS. & JUD. PRO. § 10-4B-03.
[92] MD. CODE ANN., CRIM. PRO. § 1-203(a)(1).
[93] *Id.*
[94] *See* Jones v. United States, 168 A.3d 703, 707 (D.C. Ct. App. 2017).
[95] *Id.*

using a simulator to locate a phone violated the Fourth Amendment," and (2) applying the exclusionary rule "would not meaningfully deter police misconduct."[96]

While the *Jones* court recognized that the Supreme Court upheld the good faith exception when officers reasonably believed a warrant was valid, the *Jones* court found that the police, "not acting pursuant to a seemingly valid warrant, statute, or court opinion, conducted an unlawful search using a secret technology that they had shielded from judicial oversight and public scrutiny."[97] Though *Jones* was decided several months after *Copes*, the *Jones* holding highlighted the deficiencies in the Court of Appeals' decision to consider a pen register as the functional equivalent of a warrant.

2. Misleading the issuing magistrate through omission of information disclosed in a pen register order precludes applicability of the good faith exception

Even if a pen register order were functionally the same as a warrant, the good faith exception remains inapplicable because the officers in *Copes* failed to disclose their planned use of a Hailstorm device when applying for that order.[98] The *Jones* court made a similar determination, finding that "assuming the police believed the warrantless use of the [cell site] simulator to be lawful, they could not have reasonably relied on that belief, given the secrecy surrounding the device."[99] The circumstances at play in *Copes* and *Jones*, where law enforcement officers were precluded from disclosing cell site simulator use in applications to the

[96] *Id.* at 719 (internal quotations omitted).
[97] *Id.* at 720.
[98] *Copes*, 165 A.3d at 429.
[99] *Jones*, 168 A.3d at 720.

court,[100] mirror the first circumstance in which the good faith exception to the exclusionary rule is inapplicable under *Leon*: where "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."[101] In *Copes*, as in *Jones*, law enforcement "shielded" "secret technology" from both "judicial oversight and public opinion."[102]

The *Copes* court acknowledged that the officers "failed to go into greater detail about [the] technology" the officers planned to use, but ultimately found that "search warrants need not 'include a specification of the precise manner in which they are to be executed.'"[103] The Court of Appeals relied on the Supreme Court's holding in *Dalia v. United States* that law enforcement officers need not enumerate in precise detail the officers' intended surveillance method, even in a warrant application.[104] The *Copes* court reasoned that *Dalia* allowed for a certain level of nondisclosure: "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."[105] The *Copes* court held 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 technical details*)."[106]

---

[100] *Copes*, 165 A.3d at 446; *Jones*, 168 A.3d at 719.
[101] *Leon*, 468 U.S. at 923.
[102] *Jones*, 168 A.3d at 720.
[103] *Copes*, 165 A.3d at 446 (quoting Dalia v. United States, 441 U.S. 238, 257 (1979) (holding that under the Fourth Amendment, search warrants need not "include a specification of the precise manner in which they are to be executed").
[104] Dalia v. United States, 441 U.S. 238, 257 (1979).
[105] *Copes*, 165 A.3d at 446–447.
[106] *Id.* at 446 (emphasis added).

However, these "technical details"[107] are the thrust of the issue in *Copes*, and failing to disclose those details amounts to "[misleading the magistrate] by information in the application for the warrant that the officer knew was false or would have known was false" under *Leon*.[108] If the technical details in question may affect the issuing judge's analysis of the reasonableness of the order under the Fourth Amendment,[109] then absence of those details may mislead the issuing magistrate and render the order "fatally deficient."[110]

When applying for a warrant, the Fourth Amendment requires law enforcement to state the "place to be searched."[111] In *Copes*, that "place" was the location of Copes' cell phone. Even the less stringent pen register order application requires 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."[112] Again, in *Copes*, the

---

[107] *Id.*

[108] *Id.* at 433 (citing *Leon*, 468 U.S. at 923).

[109] "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.'" *Copes*, 165 A.3d at 447 (JJ. Hotten, Greene, and Adkins, dissenting) (quoting *Andrews*, 134 A.3d at 338).

[110] *Leon*, 468 U.S. at 923. *But see Copes*, 165 A.3d at 447 ("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.").

[111] U.S. CONST., amend. IV.

[112] MD. CODE ANN., CTS. & JUD. PRO. § 10-4B-03(b)(2).

"information likely to be obtained" is the location of the cell phone.[113]

Significantly, however, depending on the technology used—CSLI or cell site simulator—"location" has two discrete meanings: *approximate location* and *precise location*. A traditional pen register (and related technology, the trap and trace), uses information gathered from a third-party service provider to generate a list of various signals transmitted to and from a specific phone.[114] Using a pen register order to access CSLI, at issue in *Carpenter*, is a way to determine a cell phone's *approximate location* by triangulating the radial range of the existing cell phone towers from which the phone derives its communicative capability.[115]

Conversely, a cell site simulator, at issue in *Copes*, is a device with which law enforcement officers may simulate a cell phone tower themselves.[116] Therefore, law enforcement does not use information from existing cell towers to capture a specific phone number to immediately identify the *precise location* of the phone associated with that number.[117] Using a cell site simulator achieves a more specific result than relying on a traditional pen register or CSLI. As such, the location results—the "place to be searched" under the Fourth Amendment—when using a cell site simulator rather than CSLI are qualitatively different.[118] Thus, failing to disclose planned use of a cell site simulator when applying for a pen register order may have substantial effects on the issuing judge's reasonableness analysis.[119] In failing to disclose, law

---

[113] *Id.*
[114] 18 U.S.C. §§ 3127(3), 3127(4) (2012).
[115] Carpenter v. United States, 585 U.S. —, slip op. at 2 (2018).
[116] *See* Fenton, *supra* note 6.
[117] *Id.*
[118] U.S. CONST. amend. IV.
[119] *Leon*, 468 U.S. at 923.

enforcement puts a thumb on the scale in its favor in a way that should render a resulting pen register order invalid under *Leon*.[120]

The officers in *Copes* did not mention their planned use of a cell-site simulator in their application for a pen register order because a nondisclosure agreement between Hailstorm's manufacturer and the Baltimore Police Department bound those officers to silence on the subject, even to judges.[121] This failure to disclose the use of a cell-site simulator is evidence of "reckless disregard for the truth" about the technology's uses and capabilities.[122] The "technical details"[123] of a Hailstorm device are qualitatively different and more advanced than other means by which law enforcement may "initiate a signal to determine the location of the subject's mobile phone."[124] For example, a Hailstorm device can remotely make a targeted phone ring.[125] These crucial distinctions (1) affect the efficacy and quality of the information gathered; and (2) may affect an issuing judge's analysis. Thus, allowing for a good faith exception to the Fourth Amendment violation in *Copes* was inappropriate.

---

[120] *Id.*
[121] *Copes*, 165 A.3d at 452. *See also* Fenton, *supra* note 6; Ernest Reith, Letter to Police Commissioner Bealefeld and State's Attorney Bernstein, *Purchase Wireless Collection Equipment/Technology and Non-Disclosure Obligation*, Federal Bureau of Investigation (July 13, 2011), http://www.baltimoresun.com/bal-police-stingray-non-disclosure-agreement-20150408-htmlstory.html.
[122] *Leon*, 468 U.S. at 923.
[123] *Copes*, 165 A.3d at 446.
[124] *Id.*
[125] *See* Fenton, *supra* note 6.

C. The Court of Appeals should have employed the rational precedent set forth in *Andrews*

Despite its finding that Copes' Fourth Amendment rights were likely violated, the Court of Appeals declined to apply *State v. Andrews*.[126] *Andrews* is a Maryland Court of Special Appeals case that involved the precise type of surveillance technology that law enforcement utilized in *Copes*.[127] The facts in *Copes* and *Andrews* related to law enforcement's behavior are largely in synthesis.[128] The law enforcement officers in *Andrews* were subject to a nondisclosure agreement between the Federal Bureau of Investigation and the State's Attorney's Office.[129] Police officers in *Copes* were also bound not to disclose use of the Hailstorm device in pen register applications.[130] The *Copes* court noted that "[w]ith respect to the nondisclosure agreement . . . the testimony at the hearing in *this* case was that the detectives would have answered any questions of the issuing judge about what they

---

[126] State v. Andrews, 134 A.3d 324, 327 (Md. App. 2016) (affirming a prior decision to suppress evidence gained using a cell cite simulator).
[127] *Id.*
[128] *Copes*, 165 A.3d at 438 ("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.") (citing *Andrews*, 134 A.3d at 327-29).
[129] *Id.* at 446.
[130] *See* Fenton, *supra* note 6.

planned to do."[131] Because officers would have answered questions about the Hailstorm device were they asked about that device, the *Copes* court found no bad faith.[132]

The *Copes* court correctly pointed out that *Andrews* cites *United States v. Graham*, a case that the Fourth Circuit overruled *en banc*.[133] Upon re-hearing, the full Fourth Circuit panel in *Graham* held that acquisition of CSLI without a warrant is covered by the good faith exception.[134] However, the type and specificity of the location information gathered sufficiently distinguish CSLI and cell site simulators.[135] As CSLI and cell site simulators are distinguishable, so too are the situations in *Graham*, *Andrews*, and later *Copes*. Moreover, *Graham* has been abrogated by the Supreme Court's decision in *Carpenter*, holding that law enforcement must obtain a warrant before acquiring CSLI data.[136]

Finally, the *Copes* court's assertion that "the detectives would have answered any questions of the issuing judge about what they planned to do"[137] unreasonably stretches the *Leon* Court's rule against misleading a magistrate.[138] The *Copes* court found that so long as officers are willing to answer an issuing judge's questions, those officers did not mislead that judge by omitting details.[139] However, the officers in *Copes* withheld highly pertinent

---

[131] *Copes*, 165 A.3d at 446.
[132] *Id.*
[133] *Id.* at 439; *see also* United States v. Graham, 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted by* United States v. Graham, 824 F.3d 421 (4th Cir. 2016), *abrogated by* Carpenter v. United States, 585 U.S. — (2018).
[134] United States v. Graham, 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted by* United States v. Graham, 824 F.3d 421 (4th Cir. 2016), *abrogated by* Carpenter v. United States, 585 U.S. — (2018).
[135] *See supra* Part II.B.ii.
[136] Carpenter v. United States, 585 U.S. —, slip op. at 21 (2018).
[137] *Copes*, 165 A.3d at 446.
[138] *Leon*, 468 U.S. at 923.
[139] *Copes*, 165 A.3d at 446.

information from the issuing judge when applying for a pen register order, specifically, the crucial information regarding how the officers planned to execute their surveillance.[140] Finding that law enforcement's later willingness to answer questions negated any bad faith expressed by withholding information from the magistrate unreasonably stretches the factors in *Leon*,[141] transferring law enforcement's burden to issuing judges. Such a finding effectively requires judges to proactively ask officers questions about the very technology those officers omit from their pen register orders. Judges, then, may not be aware of what questions to ask, precisely because officers withhold their use of Hailstorm devices.

CONCLUSION

Conflation of the nature and function of related but distinct emerging technologies, particularly when used by law enforcement, is a misapplication of facts to relevant law that can result in injustice, as in *Copes*. The good faith exception to the exclusionary rule should be construed narrowly, particularly when the use and disclosure of details of surveillance technology are involved. A narrow construction of the good faith exception allows for more effective preservation of privacy rights in the twenty-first century.

---

[140] *Id.*
[141] *Leon*, 468 U.S. at 923.