PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 18-1953

KERRON D. ANDREWS,

Plaintiff – Appellant,

v.

BALTIMORE CITY POLICE DEPARTMENT; KEVIN DAVIS, Commissioner; MICHAEL SPINNATO, Detective; JOHN HALEY, Detective,

Defendants – Appellees,

L3HARRIS TECHNOLOGIES, INC.,

Intervenor.

Appeal from the United States District Court for the District of Maryland, at Baltimore. Stephanie A. Gallagher, District Judge; Catherine C. Blake, Retired District Judge. (1:16-cv-02010-CCB)

Argued: January 27, 2026 Decided: September 24, 2026

Before QUATTLEBAUM, HEYTENS, and BERNER, Circuit Judges.

Affirmed by published opinion. Judge Berner wrote the opinion, in which Judge Heytens joined. Judge Quattlebaum wrote an opinion concurring in part and in the judgment.

ARGUED: Michael A. Pichini, GOODELL, DEVRIES, LEECH & DANN, Baltimore, Maryland, for Appellant. Natalie Rose Amato, BALTIMORE CITY LAW DEPARTMENT, Baltimore, Maryland, for Appellees. **ON BRIEF:** James B. Astrachan,

H. Mark Stichel, Elizabeth A. Harlan, Trisha L. Scott, ASTRACHAN GUNST THOMAS, P.C., Baltimore, Maryland; Michael C. Heyse, George S. Mahaffey, GOODELL, DEVRIES, LEECH & DANN, Baltimore, Maryland, for Appellant. Andre M. Davis, City Solicitor, Ebony M. Thompson, City Solicitor, Brent D. Schubert, Deputy Chief, Michael P. Redmond, Chief Solicitor, Rachel A. Simmonsen, Assistant Solicitor, BALTIMORE CITY LAW DEPARTMENT, Baltimore, Maryland, for Appellees.

BERNER, Circuit Judge:

While investigating a shooting, Baltimore City Police Department detectives obtained a warrant for the arrest of a suspect, Kerron Andrews. They also obtained a court order to allow them access to certain records from Andrews's cellphone provider. Using records received from the provider, the detectives were able to narrow down Andrews's location to a few city blocks. They then used a device known as a cell-site simulator to track the location of Andrews's cellphone to a specific townhome. Cell-site simulators prompt all nearby cellphones to automatically send an electronic signal to the simulator, thereby revealing the location of each cellphone and, in most instances, the location of the cellphone's owner. With the consent of the resident, the detectives entered the townhome. There they found Andrews sitting on a couch with his cellphone in his pocket.

Following a search of the townhome, prosecutors brought criminal charges against Andrews. The detectives' use of the cell-site simulator was only revealed to Andrews's counsel a year after the criminal proceedings against him began. Following this revelation, Andrews moved to suppress the evidence obtained through the use of the simulator. Both the Maryland trial and appellate courts ruled that the detectives' use of the cell-site simulator without a warrant violated Andrews's Fourth Amendment rights. The charges against Andrews were subsequently dismissed, and he was released after spending nearly two years in pretrial detention.

Andrews subsequently filed this civil lawsuit seeking damages for the violation of his federal and state constitutional rights. A district court granted summary judgment to the defendants, finding as a matter of law that Andrews's constitutional rights had not been

violated. A different panel of this court reversed and remanded to the district court for discovery. After discovery, the district court once again entered summary judgment on behalf of the defendants. The case now returns to our court.

We hold that the use of the cell-site simulator constituted a search within the meaning of the Fourth Amendment. We conclude, however, that the detectives are entitled to qualified immunity and state law public official immunity, and that the Baltimore City Police Department cannot be held liable for the violation of Andrews's Fourth Amendment rights. We therefore affirm the district court's grant of summary judgment to the defendants.

I. Cell-Site Simulators

This case involves the use of a little-known—though long-utilized—technology called a cell-site simulator. We begin by explaining this technology.

Cell sites are a "set of radio antennas" that create a wireless network and provide the signals that cellphones rely on to function. *Carpenter v. United States*, 585 U.S. 296, 300 (2018). "Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features." *Id.* at 300–01. When a phone connects to a cell site, "it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site." *Id.* at 301. CSLI supplies a cellphone provider with the equivalent of historical and real-time location data for all cellphones in the provider's network.

A cell-site simulator functions by essentially "impersonat[ing]" an actual cell site. *Andrews v. Balt. City Police Dep't*, 8 F.4th 234, 235 (4th Cir. 2020) (*Andrews I*). "In response to signals emitted by the simulator, every cell phone and other cellular-enabled device in the area [using the same service provider] identifies the simulator as the best local cell tower and transmits a connection signal containing that device's unique identifier to the simulator." *Id.* Through the use of a handheld cell-site simulator, law enforcement can "home in on the location of a suspect's cell phone by moving around an area while observing the strength and direction of the phone's signal." *Id.* In this way, cell-site simulators enable law enforcement to determine the location of an individual cellphone without seeking information from the cellphone provider. This location data, which is available instantly and in real time, is generally more precise than CSLI.

The Baltimore City Police Department (BPD), like other law enforcement agencies around the country, has used cell-site simulators for decades.[1] Hailstorm, the specific cell-site simulator at issue in this case, is manufactured by L3Harris (previously the Harris Corporation). The BPD obtained Hailstorm, and its predecessor, Stingray, from the Federal Bureau of Investigation.

[1] In 2004, an episode of the television show *The Wire* portrayed a Baltimore police officer using a cell-site simulator called a "Triggerfish" to monitor a suspect's cell phone activity. The Wire, Season 3, Episode 11: *Middle Ground* (HBO Max, accessed Sep. 17, 2026); *see also* Jessica Anderson, *Sun Investigates: Cellphone surveillance seen years earlier in 'The Wire'*, Balt. Sun (Apr. 11, 2015), www.baltimoresun.com/2015/04/11/sun-investigates-cellphone-surveillance-seen-years-earlier-in-the-wire/ [https://plus.lexis.com/api/permalink/f83b7c00-484e-4359-923b-1700f49159e0/].

As a condition for acquiring Hailstorm, the FBI required the BPD to enter into a non-disclosure agreement (NDA). The NDA between the FBI and the BPD obligates the BPD to "immediately notify the FBI" before it discloses the "use or provide any information" about Hailstorm in criminal or civil proceedings and to avoid such disclosure "without the prior written approval of the FBI." Parties' Joint Appendix (J.A.) 120. In other words, the NDA requires the BPD to keep its use of the cell-site simulator secret from litigants and courts unless the BPD first notifies and receives approval from the FBI. This notification is designed to provide the FBI an opportunity to "intervene to protect the equipment/technology and information from disclosure and potential compromise." *Id.* The NDA also requires "the Office of the State's Attorney for Baltimore [to], at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to provide, any information concerning the Harris Corporation wireless collection equipment/technology[.]" *Id.* at 121.

This case calls upon us to consider the constitutional restraints on the BPD's use of cell-site simulators.

II. Factual Background

On review of a grant of summary judgment, we view the facts in the light most favorable to the nonmovant. *Aleman v. City of Charlotte*, 80 F.4th 264, 293 (4th Cir.

2023).[2] Here, the parties largely agree on the relevant facts. They dispute the legal determinations arising out of those facts.

A. Pen Register Order

In 2014, the BPD began to suspect that Kerron Andrews, a young man who had previously worked with them as an informant, had been involved in a recent shooting that injured three people. The BPD obtained an arrest warrant charging Andrews with attempted murder. Three days later, unable to determine where Andrews lived, BPD Detective Michael Spinnato, one of the defendants in this case, sought a pen register order from the Circuit Court for Baltimore City.

A pen register is a device or process that phone companies can use to record the telephone numbers dialed from a specific telephone line.[3] *See, e.g.*, 18 U.S.C. § 3127(3) (defining pen register for purposes of federal law); Md. Code Ann., Cts. & Jud. Proc. (CJP) § 10-4B-01(c) (defining pen register for purposes of Maryland law). Importantly, though a pen register captures a record of incoming and outgoing telephone calls, it does not record the content of the calls. A pen register order (PRO) is a court order that requires a phone

[2] Andrews argues that the district court did not present the facts in the light most favorable to him in its description of the technology. We review the grant of summary judgment *de novo* and present the facts in the light most favorable to Andrews, as we are obliged to do.

[3] In the past, phone companies had to install a physical device to collect this data. As a result, a pen register would include only a record of telephone calls going forward. As technology has evolved, however, phone companies no longer need to rely on a physical tool. Phone companies now generally maintain a record of all incoming and outgoing phone calls of every phone.

company to provide law enforcement a copy of an individual's records of incoming and outgoing phone calls.

Because of its "limited capabilities"—providing only a list of phone calls—the Supreme Court has held that the use of a pen register device is not a "search" within the meaning of the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735, 742–46 (1979). In seeking a PRO, therefore, law enforcement need not meet the heightened standard required by the Fourth Amendment to issue a valid warrant—namely, probable cause that "contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The only requirements to obtain a PRO, therefore, are those set out in the relevant federal statutes and state law. Meeting these requirements is generally not onerous. To issue a PRO in Maryland, a court need only find that "the information likely to be obtained by the installation and use [of the device] is relevant to an ongoing criminal investigation." CJP § 10-4B-04(a)(1); *see also* 18 U.S.C. § 31239(a) (providing that a federal court shall issue a PRO if the court finds that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation").

In applying for the PRO for Andrews's cellphone data, Detective Spinnato attested that a pen register was necessary to "assist in the apprehension of" Andrews. J.A. 30. Detective Spinnato certified that "the information likely to be obtained concerning [Andrews's] location will be obtained by learning the numbers, locations and subscribers of the telephone number(s) being dialed or pulsed from or to [Andrews's] telephone and that such information is relevant to the ongoing criminal investigation being conducted by the Agency." *Id.* Detective Spinnato further certified that "probable cause exists based

upon the information supplied in this application, that [Andrews] is using the cellular phone number [listed in the application] for criminal activity and that the application will lead to evidence of the crime(s) under the investigation." *Id.* at 38.

A Maryland magistrate granted the request for the PRO, authorizing the government to obtain information about Andrews's cellphone for a period of sixty days. The PRO stated:

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

Id. at 39. The PRO required Andrews's cellphone provider to turn over information about Andrews's cellphone, including the equivalent of the phone's electronic serial number.

The PRO required the provider to give the detectives "up to 24 months of prior detailed call history[.]" *Id.* at 42. In addition, borrowing the exact language used by Detective Spinnato in his application, the PRO required the provider to supply an array of specialized data, including "cell site information of the aforesaid target telephone, Historical Global Position System Tracing and Tracking, Mobile Locator tools, R.T.T. (Real Time Tracking Tool), . . . Precision Locations[,] and any and all locations only if requested by the Agency." *Id.* at 42–43. The PRO, again adopting Detective Spinnato's language, further permitted the detectives to "employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of a Pen Register" and to "initiate a signal to determine the location of the subject's mobile device. . . ." *Id.* at 40.

B. Use of the Hailstorm Cell-Site Simulator

On the same day that the magistrate issued the PRO, Andrews's cellphone provider, Sprint Communications, began to supply data about Andrews's cellphone to the BPD. The data included the cellphone's identifying information, thirty days of historical CSLI, sixty days of pen register data (incoming and outgoing call history), and recent GPS coordinates. *State v. Andrews*, 134 A.3d 324, 328–29 (Md. Ct. Spec. App. 2016).

The GPS coordinates showed the past location of Andrews's phone "within a . . . 200 to 1600 meter radius[.]" *Id.* at 329. Based on this data, the BPD concluded that Andrews's phone had been located somewhere near the 5000 blocks of Clifton Avenue in Baltimore City. *Id.* These blocks contain approximately thirty-five townhomes, and the BPD were unable to obtain a more precise location for Andrews's cellphone. *Id.* Detective John Haley, a member of the BPD's Advanced Tactical Team (ATT) and a defendant in this case, proceeded to use a Hailstorm cell-site simulator in an effort to locate Andrews. A group of law enforcement officers, including Detectives Haley and Spinnato, walked up and down the 5000 blocks of Clifton Avenue until the simulator connected with Andrews's cellphone, pinpointing its location within a specific townhome.

Detective Spinnato knocked on the door of the townhome and, after obtaining consent from the woman who answered, went inside. There he found Andrews sitting on a couch in the living room with his cellphone in his pocket. The officers detained Andrews. While in the townhome, they obtained and executed a search warrant. During the search,

the officers discovered a gun stuffed between the cushions on the couch where Andrews had been sitting.

Despite repeated questions from Andrews's counsel concerning the search of the townhome, the prosecution did not disclose the use of Hailstorm to locate Andrews until a year into Andrews's criminal case. *See id.* at 329–30. Following the disclosure, Andrews moved to suppress evidence obtained by the use of Hailstorm, and the Maryland trial court granted the motion. *Id.* at 333–34. The prosecution appealed that ruling to Maryland's intermediate court, which affirmed the suppression ruling. *Id.* at 365.

The Maryland intermediate court, as a matter of first impression, held that the use of Hailstorm to locate Andrews constituted a "search" within the meaning of the Fourth Amendment because of the simulator's ability to "locate and track the movements of a cell phone and its user across both public and private spaces." *Id.* at 348. Given that the Fourth Amendment applied, the officers needed a warrant in order to use the cell-site simulator. The Maryland intermediate court ruled, also as a matter of first impression, that the Maryland Pen Register Statute is "limited by its terms and is not intended to apply to other, newer technologies" like cell-site simulators. *Id.* at 356–57. The intermediate court rejected the prosecution's argument that the PRO was functionally equivalent to a search warrant. *Id.* at 358–60. Finally, the intermediate court determined that the good faith exception to the warrant requirement did not apply.[4] *Id.* at 363–65. Accordingly, the Maryland

[4] Under the good faith exception, "evidence obtained by an officer who acts in objectively reasonable reliance on a search warrant will not be suppressed, even if the warrant is later deemed invalid" unless the warrant is so facially invalid that a reasonable (Continued)

intermediate court affirmed the exclusion of evidence obtained by the BPD through the use of the Hailstorm cell-site simulator. *Id.* at 365. The prosecution dropped the criminal case against Andrews.

III. Procedural Background

Shortly after his criminal case was dismissed, Andrews brought this Section 1983 civil rights action against the BPD, the Commissioner of the BPD in his official capacity, and BPD Detectives Spinnato and Haley in their official and individual capacities (collectively the Defendants). *See* 42 U.S.C. § 1983. Andrews alleges that Detectives Spinnato and Haley violated his rights under the Fourth and Fourteenth Amendments of the United States Constitution and the Maryland Declaration of Rights through their use of the cell-site simulator. He also alleges that the BPD and the BPD Commissioner are responsible for the purported constitutional violations by enacting or perpetuating an unconstitutional policy to permit and encourage the use of cell-site simulators without a warrant. Andrews filed suit in the Circuit Court for Baltimore City, seeking damages for the two years he spent in detention awaiting trial in his criminal case.[5]

---

officer would not have relied upon it. *United States v. Ray*, 141 F.4th 129, 134 (4th Cir. 2025) (quoting *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018)).

[5] Andrews also sought an injunction that would require the BPD to seek a warrant prior to using this technology. Andrews's request for injunctive relief is now moot because, subsequent to the events underlying this case, the State of Maryland enacted a law requiring law enforcement to obtain a search warrant before using a cell-site simulator to locate a suspect. *See* Md. Code Ann., Crim. Proc. § 1-203.1; *Roberts v. Engelke*, 180 F.4th 634, 642 (4th Cir. 2026) ("[T]he mootness doctrine recognizes that some intervening circumstances deprive the plaintiff of a personal stake in the outcome of the lawsuit, such (Continued)

The Defendants subsequently removed the case to federal court and then moved to dismiss. The district court converted the Defendants' motion to dismiss to a motion for summary judgment, which it granted. The district court concluded that the PRO "objectively authorized the use of a cell-site simulator," and, therefore, there was no constitutional violation. *Andrews v. Balt. City Police Dep't*, No. CV CCB-16-2010, 2018 WL 3649602, at *9 n.9 (D. Md. Aug. 1, 2018).

Andrews appealed and a different panel of this court remanded for the limited purpose of discovery on six specific questions: 1) the range at which the simulator can prompt nearby cellular devices to connect to it; 2) the maximum number of devices with which the simulator can connect; 3) the categories of data collected from the cellphones; 4) the data stored by Hailstorm; 5) the data accessible to law enforcement officers; and 6) the means by which Hailstorm was configured to minimize data collection from third party cell devices not belonging to Andrews. *Andrews I*, 8 F.4th at 238. The court also directed the district court to make factual findings "as to whether—aside from the non-disclosure agreement between BPD and the FBI—BPD had, at the time of its application for the [PRO], any formal or informal policies, practices, or procedures that prevented BPD officers seeking a warrant or pen register/trap and trace order from stating to the reviewing magistrate that a cell site simulator would be used." *Id.* The court retained jurisdiction. *Id.* at 235.

---

that the action can no longer proceed." (quoting *Synopsys, Inc. v. Risk Based Sec., Inc.*, 70 F.4th 759, 764 (4th Cir. 2023))).

On remand, Andrews moved to compel discovery of an operator's manual for Hailstorm, arguing that it was necessary to answer the panel's questions. The district court denied the request.[6] At the close of discovery, three years after that denial, the Defendants moved for summary judgment. The district court made findings of fact in response to each of the questions posed in *Andrews I*. *Andrews v. Balt. City Police Dep't*, No. CV SAG-16-2010, 2025 WL 876711, at *3–10 (D. Md. Mar. 19, 2025). Because this court had retained jurisdiction, however, the district court was precluded from ruling on the Defendants' motion for summary judgment. *Id.* at *10. The case then returned to this court for further adjudication. *Id.*

In April 2025, this court again sent the case back to the district court, this time with instructions to rule on the outstanding motion for summary judgment. On remand from this court for the second time, the district court granted the Defendants' motion. *Andrews v. Balt. City Police Dep't*, No. CV SAG-16-2010, 2025 WL 1346547, at *8–10 (D. Md. May 8, 2025). The district court concluded, in the alternative, that even if the search was improper, Detectives Haley and Spinnato were entitled to qualified immunity and Maryland's public official immunity. *Id.* at *11–12. Finally, the district court found that Andrews had failed to put forth evidence to create a genuine dispute of material fact as to

[6] Among his claims on appeal, Andrews argues that the district court abused its discretion by denying his request for further discovery. We disagree. The district court permitted ample discovery. Regardless, because our ruling is based on qualified immunity, which is a question of law, further discovery on the technological capacities of Hailstorm would not change that result.

whether the BPD and Commissioner could be held liable for the alleged constitutional violation. *Id.* at *12.

Before us is Andrews's appeal from this grant of summary judgment.[7]

IV. Analysis

This court reviews a district court's grant of summary judgment *de novo*, viewing the evidence and drawing reasonable inferences in the light most favorable to the nonmovant, here, Andrews. *Henry v. Purnell*, 652 F.3d 524, 531 (4th Cir. 2011) (en banc). Summary judgment is appropriate only if a party shows that there is no genuine dispute of material fact and that they are entitled to judgment as a matter of law. *See id.*; Fed. R. Civ. P. 56(a).

We begin our analysis with the threshold question: whether the use of the cell-site simulator constituted a search for purposes of the Fourth Amendment. We then address the various defenses raised by the Defendants. We hold that the Fourth Amendment requires a valid warrant for the use of a cell-site simulator. We conclude, nonetheless, that the Defendants are entitled to summary judgment.

[7] The company that manufactures Hailstorm, L3Harris, intervened in this appeal for the limited purpose of filing a motion to seal the courtroom, which this court granted in part.

A. Constitutional Violations

Andrews alleges that the BPD violated his federal and state constitutional rights when the Defendants used the cell-site simulator to track his location inside of a residence. The Fourth Amendment to the United States Constitution, which was made applicable to the states by the Fourteenth Amendment, protects against unreasonable search and seizure by the government. U.S. Const. amend. IV. So too do Articles 24 and 26 of the Maryland Constitution. Md. Const., Declaration of Rights, arts. 24 and 26. Maryland interprets its state constitutional provisions related to search and seizure to provide the same protections as the Fourth Amendment. *See Wilson v. Prince George's County, Maryland*, 893 F.3d 213, 224 (4th Cir. 2018). We therefore analyze the claims as one.

The government conducts a search when a law enforcement officer "obtains information by physically intruding on a constitutionally protected area," which the Fourth Amendment defines as "persons, houses, papers, and effects." *United States v. Jones*, 565 U.S. 400, 406 n.3, 404 (2012). Even absent physical trespass, the government may conduct a search for purposes of the Fourth Amendment when it intrudes upon an individual's reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 351–52, 360–62 (1967). This rule is often referred to as the "*Katz* test." *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

Fourth Amendment jurisprudence endeavors to strike a delicate balance between individual privacy and public safety. It is the responsibility of the judiciary to ensure that, as "[s]ubtler and more far-reaching means of invading privacy have become available to

the Government," the "progress of science does not erode Fourth Amendment protections." *Carpenter*, 585 U.S. at 320 (internal quotation marks and citation omitted).

Among the manifold technological advances since the founding of our country, cellphones pose a unique threat to individual privacy. Cellphones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 573 U.S. 373, 385 (2014). A cellphone effectively "tracks nearly exactly the movements of its owner." *Carpenter*, 585 U.S. at 311. Accordingly, the Supreme Court has recognized that individuals have a heightened expectation of privacy both in their cellphones' contents and historical location data. *See Chatrie v. United States*, 609 U.S. ---, 146 S. Ct. 2193, 2207–09 (2026); *Carpenter*, 585 U.S. at 311; *Riley*, 573 U.S. at 394–97.

We must assess two questions. First, whether an individual has a reasonable expectation of privacy in the real-time location of his cellphone, which generally corresponds with his location. Second, whether law enforcement conducts a search by using technology that briefly seizes the cellphone's signals—unbeknownst to the owner—to track that location. Despite the ubiquity of cell-site simulators, no federal court of appeals has squarely addressed whether law enforcement's use of this technology for real-time tracking of a cellphone constitutes a search for purposes of the Fourth Amendment.[8] Today, we hold that it does.

[8] The Defendants initially conceded that the BPD's use of Hailstorm constituted a search for purposes of the Fourth Amendment. *Andrews I*, 8 F.4th at 236. Now before this (Continued)

The Supreme Court's most recent decisions on the constitutional boundaries of cellphone location surveillance, *United States v. Carpenter*, 585 U.S. 296 (2018), and *Chatrie v. United States*, 609 U.S. ---, 146 S. Ct. 2193 (2026), are instructive. Both cases were decided after the BPD used Hailstorm to locate Andrews.

In *Carpenter*, the Supreme Court considered "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements [known as CSLI]." 585 U.S. at 300. In investigating a series of robberies, the government applied for a court order to access historical CSLI from a suspect's cellphone provider. *Id.* at 301–02. In arguing that there was no Fourth Amendment search, the prosecution analogized to *Smith v. Maryland*, which established that individuals do not have a reasonable expectation of privacy in pen register data. 442 U.S. 735, 742–46 (1979). The Supreme Court rejected this argument, noting that "few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." *Carpenter*, 585 U.S. at 309. The Supreme Court made clear that an individual maintains a reasonable "anticipation of privacy in his physical location." *Id.* at 311. Accordingly, accessing historical CSLI constitutes a search for purposes of the Fourth Amendment. *Id.* at 316.

---

court for the second time, the Defendants disavow their prior concession. *See* Oral Argument at 21:47; Response Br. at 6 n.3.

Our concurring colleague suggests that we should not address whether the use of the Hailstorm was a search or whether it invaded a protected privacy interest. We disagree. Lower courts may exercise their sound discretion to determine the ordering of the qualified immunity analysis. *Pearson v. Callahan*, 555 U.S. 223, 236 (2009).

Nearly a decade later, in *Chatrie*, the Supreme Court considered a similar challenge to law enforcement's access of cellphone location data collected and stored by a third-party tech company. 146 S. Ct. at 2199. The Supreme Court reaffirmed that "an individual has a legitimate expectation of privacy in the information . . . about his cell phone's—meaning his own—movements" and that "police invade that expectation, and thus conduct a search, when they acquire that information, even though for only a limited period of time and even though via a third[ ]party." *Id.* at 2206.

The Supreme Court's rulings in both *Carpenter* and *Chatrie* were animated by concerns about the extent of the invasion of privacy provided by such tracking. Notably, CSLI allows police "'near perfect surveillance' of an individual holding a cellphone." *Id.* at 2208 (quoting *Carpenter*, 585 U.S. at 311–12). The precision of this data allows law enforcement to monitor the "comings and goings in any area" of "any number of people in any number of places, public and private[.]" *Id.*

Unlike the data obtained by law enforcement in *Carpenter* and *Chatrie*, the data collected by a cell-site simulator like Hailstorm provides only a snapshot of an individual's real-time location, rather than a log of his historical movements. Nonetheless, the use of a cell-site simulator to identify or track an individual's physical location implicates similar privacy concerns. The Supreme Court in *Chatrie* made clear that the duration of the incursion does not impact the reasonableness of an individual's expectation of privacy. Rather, "[w]here the Fourth Amendment applies, it applies—regardless of 'the quality or quantity of information' the government obtains." *Id.* at 2210 (quoting *Kyllo*, 533 U.S. at 37).

This case demonstrates the relative invasiveness of cell-site simulator technology. First, the location information provided by the cell-site simulator was more precise than the real-time location data that Detectives Haley and Spinnato obtained from Andrews's cellphone provider. *See id.* at 2208 (comparing the ability of a cellphone provider's CSLI data to pinpoint a suspect within "one-eighth to four square miles" with the ability of a tech company's cellphone location data to pinpoint a suspect's location within "around twenty meters" (citation omitted)). Here, the Detectives relied upon the CSLI obtained from Andrews's cellphone provider to narrow down his location to a few city blocks. When Detectives Haley and Spinnato could not pinpoint in which townhome Andrews was located from this data, they turned to the cell-site simulator. Following the Supreme Court's rulings in *Carpenter* and *Chatrie*, law enforcement officers would have needed to obtain a warrant to access CSLI and comparable data. This principle applies equally to a technology that can provide even more precise information about an individual's location.

Furthermore, the cell-site simulator was used to track Andrews *inside* a private residence. The privacy of the home holds special importance in Fourth Amendment jurisprudence. "[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." *United States v. Karo*, 468 U.S. 705, 714 (1984). Surveillance that passes from public streets into private homes has long been recognized to convert a permissible law enforcement tactic into a Fourth Amendment search. *Compare United States v. Knotts*, 460 U.S. 276, 281 (1983) (finding that the use of a beeper to tail a car did not constitute a search because the car was always

"in plain view" (citation omitted)), *with Karo*, 468 U.S. at 716 (finding that the same technology brought into a private residence could constitute a Fourth Amendment search).[9]

While a cell-site simulator may only provide limited information, it is likely to "reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant." *Karo*, 468 U.S. at 715. This technology is akin to sense-enhancing technology that allows the government to peer into a private home, which the Supreme Court has repeatedly held requires a warrant. *See id.* at 714 (granting a motion to suppress evidence obtained from warrantless use of a GPS device to monitor a private residence "not open to visual surveillance"); *Kyllo*, 533 U.S. at 37 (finding that warrantless use by law enforcement of sensory-enhancing technology to trace heat signatures in a home violated the Fourth Amendment). The cell-site simulator here effectively "crack[ed] open the front door" of the townhome to reveal Andrews inside. *Kyllo*, 533 U.S. at 37.

Furthermore, while *Carpenter* and *Chatrie* dealt with the government's ability to access location data that individuals voluntarily share with private third parties, the BPD used Hailstorm to collect location information directly. *See Carpenter*, 585 U.S. at 309–10, 314 (distinguishing between the expectations of privacy related to information

[9] The Seventh Circuit held, prior to *Chatrie*, that law enforcement's use of live cell-site location information obtained from a cellphone provider did not constitute a Fourth Amendment search. *See United States v. Hammond*, 996 F.3d 374, 391–92 (7th Cir. 2021). In its ruling, the Seventh Circuit stressed that the facts in that case did "not suggest that law enforcement used either the real-time CSLI . . . to examine the defendants' movements inside of a home or other highly protected area." *Id.* at 389. Here, that is exactly what the BPD did with its use of Hailstorm.

willingly shared with a third party and information obtained solely by the government through its own surveillance techniques). The cell-site simulator functions by taking control of the suspect's phone, albeit briefly. When Hailstorm connects to a cellphone, the cellphone's owner is unable to receive phone calls (other than a 911 call) or text messages. In addition to the suspect's cellphone, Hailstorm connects with—and therefore temporarily renders inoperable—all cellphones in the area that rely on the same cellular service provider.

We agree with the Maryland intermediate court that Andrews had an objectively reasonable expectation that his "cell phone[] will not be used as [a] real-time tracking device[] through the direct and active interference of law enforcement." *Andrews*, 134 A.3d

at 350. We therefore conclude that the use of a cell-site simulator constitutes a search, deserving of the protection of the Fourth Amendment.[10]

B. Defenses to Liability

Our inquiry does not end there. The Defendants raise a number of defenses that they argue nonetheless preclude a ruling in Andrews's favor: qualified immunity, public official immunity, and *Monell* liability. Qualified immunity shields individual law enforcement officers from civil liability when, in light of clearly established law, they could reasonably have believed that their actions were lawful. *Henry*, 652 F.3d at 531. Maryland's public

[10] The Defendants argue that, even if the use of Hailstorm constituted a search, the search was authorized by the PRO. Andrews contends that the PRO does not satisfy the warrant requirement of the Fourth Amendment. Our concurring colleague agrees with the Defendants that the PRO satisfied the warrant requirement. The Maryland state trial and intermediate courts disagreed, concluding that orders issued under the Maryland Pen Register statute cannot authorize the use of a cell-site simulator and furthermore that the order obtained in Andrews's case was not the functional equivalent of a warrant. *Andrews*, 134 A.3d at 354–61. We need not reach the issue of whether the PRO satisfied the warrant requirement, however. As we explain below, we conclude that the Defendants are entitled to summary judgment given the lack of precedent establishing that the use of a cell-site simulator constitutes a Fourth Amendment search.

Moreover, law enforcement in Maryland can no longer rely on PROs as a permissible mechanism to obtain authorization for the use of a cell-site simulator. Several months after the BPD used Hailstorm to locate Andrews, Maryland's legislature passed a law in 2014 mandating that law enforcement obtain a warrant before using a cell-site simulator. *See* Md. Code Ann., Crim. Proc. § 1-203.1. In 2015, just over one year after Andrews's arrest, Congress launched a bi-partisan congressional investigation that prompted the Department of Justice to similarly establish an official policy that, moving forward, federal law enforcement officials must seek a warrant before using this technology in a criminal investigation. *See* U.S. Dep't of Just., *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators* (Sept. 3, 2015), http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators [https://perma.cc/2B7G-PNLN].

official immunity similarly limits the liability of Maryland public officials from state-law claims unless the public official acted with "malice or gross negligence." *Gelin v. Maryland*, 132 F.4th 700, 707 (4th Cir. 2025) (citation omitted). Finally, though municipalities do not have immunity from suit under 42 U.S.C. § 1983, their liability for violations of constitutional rights is cabined to situations where the municipality's own "custom, policy, or practice" caused the violation. *Owens v. Balt. City State's Att'ys Off.*, 767 F.3d 379, 402 (4th Cir. 2014). This doctrine has come to be known as *Monell* liability. The Defendants assert that each of these doctrines applies here. We agree.

We begin by discussing whether Detectives Haley and Spinnato are entitled to qualified immunity and public official immunity for their use of the cell-site simulator. We then consider whether the BPD and Commissioner are entitled to summary judgment because there is not a genuine issue of material fact as to whether a municipal policy, practice or custom caused the violation.

i. Qualified Immunity

Qualified immunity is "an affirmative defense to liability where a defendant makes a decision that, even if constitutionally deficient, reasonably misapprehends the law governing the circumstances . . . confronted." *Case v. Beasley*, 167 F.4th 651, 662 (4th Cir. 2026) (quoting *Taylor v. Riojas*, 592 U.S. 7, 8 (2020)). Having concluded that Andrews's Fourth Amendment rights were violated, we turn to whether the constitutional right at issue was clearly established at the time of the violation. A constitutional right is considered clearly established when it is "sufficiently clear that every reasonable official would have understood that what he is doing violates that right." *Mullenix v. Luna*, 577 U.S. 7, 11

(2015) (quoting *Reichle v. Howards*, 566 U.S. 658, 664 (2012)). We look to "decisions of the United States Supreme Court and our own court" as well as decisions of our sister circuits to determine whether a constitutional right is clearly established. *Case*, 167 F.4th at 662. Because Andrews's constitutional right was not well-established, Detectives Haley and Spinnato are entitled to qualified immunity.

Fourth Amendment jurisprudence has understandably struggled to keep pace with rapidly evolving technology. Though this technology has been used by law enforcement agencies for decades, this court has mentioned cell-site simulators in a handful of prior cases, none of which addressed the constitutional limits of their use. *See United States v. Graham*, 824 F.3d 421, 427 (4th Cir. 2016) (en banc) (discussing the need for a warrant to use cell-site simulators in a footnote), *abrogated on other grounds by Carpenter v. United States*, 585 U.S. 296 (2016); *Andrews I*, 8 F.4th at 235 (describing cell-site simulators); *Leaders of a Beautiful Struggle v. Balt. City Police Dep't*, 2 F.4th 330, 347 (4th Cir. 2021) (en banc) (identifying cell-site simulators as part of the mass surveillance systems in the City of Baltimore); *United States v. Briscoe*, 101 F.4th 282, 294–96 (4th Cir. 2024) (finding that a court order issued pursuant to Md. Code Ann., Crim. Proc. § 1–203.1(b)(1)(ii) constitutes a valid search warrant authorizing the use of a cell-site simulator); *United States v. Wilford*, 689 F. App'x 727, 730 (4th Cir. 2017) (per curiam) (finding that the defendant lacked standing to challenge the use of a cell-site simulator authorized by a PRO). The

Supreme Court has never addressed this question, and a survey of cases from other circuits similarly shows a lack of clear guidance.

Andrews's criminal case marked the first time a Maryland appellate court addressed whether the use of a cell-site simulator constitutes a search within the meaning of the Fourth Amendment. While legislative action and policy changes have helped clarify law enforcements' obligations in using this technology, these changes occurred after the events at issue in this case.

We therefore agree with the district court that Detectives Haley and Spinnato are entitled to qualified immunity, and we affirm summary judgment on Andrews's claims against the Detectives arising under the federal Constitution.

ii. Public Official Immunity

Applying the same reasoning, we conclude that Detectives Haley and Spinnato are entitled to public official immunity for Andrews's claims arising under the Maryland State Constitution. Maryland extends immunity to public officials who "perform negligent acts during the course of their discretionary . . . duties" unless they have acted with gross negligence or malice. *Cooper v. Rodriguez*, 118 A.3d 829, 848 (Md. 2015) (citation omitted). The lack of clarity regarding whether the Detectives were required to obtain a warrant at the time coupled with the Detectives' reasonable reliance on the PRO would preclude a reasonable juror from finding that the Detectives acted with gross negligence or malice. Accordingly, we affirm the district court's grant of summary judgment on Andrews's state constitutional claims.

iii. Monell *Liability*

Andrews also named the BPD and the BPD Commissioner[11] as defendants. Municipalities and their agencies, including police departments, can be held liable for constitutional violations, including in civil rights lawsuits brought under 42 U.S.C. § 1983. *Monell v. New York City Dep't of Soc. Servs.*, 436 U.S. 658, 694 (1978). Such liability is, however, "expressly cabined." *Owens*, 767 F.3d at 402. A municipality can be liable for civil rights violations under *Monell* only if the municipality "follows a custom, policy, or practice by which local officials violate a plaintiff's constitutional right." *Id.*

Andrews alleges that the BPD maintained unconstitutional policies or practices of using cell-site simulators without first obtaining a proper warrant and of withholding information regarding the use of this technology in legal proceedings. The district court granted summary judgment to the municipal defendants, concluding that Andrews failed to produce evidence sufficient to create a genuine issue of material fact regarding the existence of such policies or practices.

In support of his arguments regarding the BPD's policies or practices, Andrews points to the NDA between the BPD and the FBI. While the NDA requires the BPD to notify the FBI before it discloses its use of Hailstorm to a court, Andrews has presented insufficient evidence to show that the requirements of the NDA were carried out in an unconstitutional manner. Rather, the Defendants put forward testimonial evidence that

[11] A suit against a government official in his official capacity is treated as a suit against the government entity itself. *Lewis v. Clarke*, 581 U.S. 155, 162 (2017). Because Andrews sued the Commissioner only in his official capacity, we consider this claim to be against the BPD itself and analyze it under *Monell*.

BPD officers understood that the NDA did not preclude them from seeking a search warrant or from disclosing the use of cell-site simulators in court. This court explicitly directed the parties to conduct discovery to identify any additional evidence to support Andrews's contention. After three years of discovery, Andrews cannot point to any evidence apart from the existence of the NDA. Having discerned no genuine dispute of material fact on this claim, we affirm the district court's grant of summary judgment to the BPD and its Commissioner.

Though we affirm the grant of summary judgment on the basis of *Monell* liability, we nonetheless echo concerns expressed by the district court that law enforcement may not rely on a private nondisclosure agreement as an excuse to conceal or obfuscate important information when seeking a search warrant or information it is required to disclose in court proceedings.

V. Conclusion

For the reasons above, we affirm the judgment of the district court.

AFFIRMED

QUATTLEBAUM, Circuit Judge, concurring in part and in the judgment:

This appeal requires us to apply principles of qualified immunity to Kerron Andrews' Fourth Amendment claims under 42 U.S.C. § 1983. As is well-settled, to overcome qualified immunity, a plaintiff must prevail on two prongs, which a court can assess in either order. *See Rambert v. City of Greenville*, 107 F.4th 388, 398 (4th Cir. 2024). One—a plaintiff must show a constitutional violation. *See id*. And two—a plaintiff must show that the right he alleges was violated was clearly established at the time of the challenged conduct. *See id*. I agree with my colleagues that the right Andrews claims the defendants violated was not clearly established. Thus, I join in affirming the district court's order granting summary judgment to the defendants. And while I think the pen register/trap & trace order (PRO) the defendants obtained satisfied the Fourth Amendment's warrant requirements, I agree that issue doesn't have to be addressed given the right Andrews claims was violated was not clearly established.

I write briefly to address two matters. First, I note some additional facts regarding the PRO. Second, I address my colleagues' findings that the defendants' use of the Hailstorm constituted a search for purposes of the Fourth Amendment and invaded privacy interests that were constitutionally protected. *See* Op. at 22–23.

On the former, it is right that the Hailstorm is not the same as a pen register/trap & trace device. But the application for the PRO specifically sought something more than a pen register/trap & trace device. It sought authorization to install and use "a device known as a Pen Register \ Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits, which registers telephone numbers

dialed or pulsed from or to" Andrews' cell phone. J.A. 28. And the application sought "authoriz[ation] to employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of" the device, that the state court authorize law enforcement 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 that the order remain in place for 60 days. *Id*. at 31. So, the Baltimore Police Department did not seek approval to install a pen register/trap & trace device and then instead use the cell site simulator. Its application to the state court referenced use of the cell site simulator.

Additionally, on probable cause, the application stated that a shooting occurred; that law enforcement identified Andrews as the suspect; that law enforcement obtained an arrest warrant for Andrews; that Detective Michael Spinnato located several possible addresses for Andrews but he wasn't found at those locations; that law enforcement confirmed Andrews' phone number; that suspects often contact family and friends for help hiding; that Andrews knew about the warrant and was evading law enforcement; that suspects generally use cell phones until their service cuts off or their phone stops working; and that tracking and monitoring Andrews' phone would assist in his apprehension. *See id*. at. 29. So, Detective Spinnato backed up his probable cause certification with specific facts.

On the latter point—my colleagues' determinations that the use of the Hailstorm was a search and invaded constitutionally protected privacy interests—those findings are made without completing prong one of the qualified immunity analysis, which must include evaluating whether the PRO was a valid warrant. And while I agree with my

colleagues that a court can award qualified immunity based on success under either prong, *see Pearson v. Callahan*, 555 U.S. 223, 236 (2009), I question the precedential value of analyzing some, but not all, of prong one, where the award of qualified immunity rests entirely on prong two, *see Payne v. Taslimi*, 998 F.3d 648, 654–55 (4th Cir. 2021) ("Dictum is a 'statement in a judicial opinion that could have been deleted without seriously impairing the analytical foundations of the holding . . . .'" (quoting *Pittston Co. v. United States*, 199 F.3d 694, 703 (4th Cir. 1999))).

In addition to being unnecessary to the clearly established conclusion, there are other reasons we shouldn't address those points. As to whether the use of the Hailstorm was a search, the defendants conceded below that it was. And neither Andrews nor the defendants appealed the district court's finding that there was a search. So, I see no need to analyze that issue. *See Hicks v. Ferreyra*, 965 F.3d 302, 310 (4th Cir. 2020) ("It is well established that this court does not consider issues raised for the first time on appeal, absent exceptional circumstances." (citation modified)).

As to the privacy interest question, I think the answer is far from clear. To me, there are significant differences between this case and *Carpenter v. United States*, 585 U.S. 296 (2018) and *Chatrie v. United States*, 609 U.S. ---, 146 S. Ct. 2193 (2026)—two of the primary cases the decision relies on. *See* Op. at 17–19. As my colleagues note, "[u]nlike the data obtained by law enforcement in *Carpenter* and *Chatrie*, the data collected by a cell-site simulator like Hailstorm provides only a snapshot of an individual's real-time location, rather than a log of his historical movements." *Id.* at 19. To me, since we're not

deciding whether there was ultimately a constitutional violation by declining to consider the PRO, we should not weigh in on this debatable issue.

In sum, because I agree that the right Andrews alleges was violated was not clearly established, I would refrain from addressing any part of prong one of the qualified immunity inquiry.*

* I also join in affirming the district court's grant of summary judgment to the defendants based on public official immunity and Andrews' failure to make out a *Monell* claim, as well as in affirming the district court's denial of Andrews' motion to compel.