PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 18-1953

KERRON ANDREWS,

Plaintiff - Appellant,

v.

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

Defendants - Appellees.

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

Argued: January 28, 2020 Decided: March 27, 2020

Before GREGORY, Chief Judge, WILKINSON and WYNN, Circuit Judges.

Remanded with instructions by published opinion. Judge Wynn wrote the opinion in which Chief Judge Gregory joined. Judge Wilkinson wrote a separate concurring opinion.

ARGUED: Henry Mark Stichel, ASTRACHAN GUNST THOMAS, P.C., Baltimore, Maryland, for Appellant. Rachel A. Simmonsen, BALTIMORE CITY LAW DEPARTMENT, Baltimore, Maryland, for Appellees. **ON BRIEF:** James B. Astrachan, Elizabeth A. Harlan, Trisha L. Scott, ASTRACHAN GUNST THOMAS, P.C., Baltimore, Maryland, for Appellant. Andre M. Davis, City Solicitor, Michael P. Redmond, Assistant Solicitor, BALTIMORE CITY LAW DEPARTMENT, Baltimore, Maryland, for Appellees.

WYNN, Circuit Judge:

Plaintiff-Appellant Kerron Andrews claims that the Baltimore Police Department ("BPD") conducted a warrantless search when it used a cell site simulator to locate him. Because the record does not contain adequate detail about the simulator's operation, we remand this matter for further factfinding.

Cell site simulators are devices that impersonate cell phone towers. *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, Dep't of Justice 2 (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download (last visited March 26, 2020). In response to signals emitted by the simulator, every cell phone and other cellular-enabled device in the area identifies the simulator as the best local cell tower and transmits a connection signal containing that device's unique identifier to the simulator. *Id.* Police officers often use handheld simulators to 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. Brian L. Owsley, *Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions*, 66 Hastings L.J. 183, 193-94 (2014).[1]

[1] Law enforcement agencies are reluctant to disclose information about cell site simulators. *United States v. Patrick*, 842 F.3d 540, 546 (7th Cir. 2016) (Wood, C.J., dissenting) (noting that the government "has gone so far as to dismiss cases and withdraw evidence rather than reveal that the technology was used"). This case is no different. In 2011, BPD entered into a non-disclosure agreement with the FBI regarding Harris Corporation's "Hailstorm" cell site simulator. The agreement strictly limited BPD from disclosing, without first consulting the FBI, "any information concerning" the Hailstorm simulator other than "the evidentiary results obtained through the use of the equipment/technology" in "pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State's case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial." J.A. 120.

In 2014, BPD used a Hailstorm cell site simulator to locate Andrews's cell phone—and thus Andrews—inside an apartment on the 5000 block of Clifton Avenue in Baltimore, Maryland. BPD used the device pursuant to a "Pen Register/Trap & Trace" order ("Pen Register Order"). The Pen Register Order did not explicitly disclose use of a Hailstorm simulator, or any other cell site simulator. Instead, it stated that police officers were "authorized to employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of a Pen Register \ Trap &Trace and Cellular Tracking Device" and "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 . . . ." J.A. 40. This language is identical to that in BPD's supporting affidavit. The Pen Register Order lasted for 60 days and was "without geographical limits." *Id.*

Defendants concede that the Hailstorm simulator searched, at minimum, Andrews's phone, and that its use thus required a warrant. Nor do Defendants controvert Andrews's assertion that the Hailstorm simulator searched other cellular devices in the vicinity, or that it searched nearby homes by transmitting spoofed cell tower signals through the walls.[2] *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (concluding that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not

[2] Although Defendants' counsel stated for the first time at oral argument that the device did not search every cellular device in the area, counsel was unable to clearly articulate the manner in which the device operated, instead acknowledging that Defendants could only reason based on "what we know" about the device's capabilities. Oral Argument at 23:10-30, https://www.ca4.uscourts.gov/OAarchive/mp3/18-1953-20200128.mp3; *see also id.* at 36:15-32, 41:02-12, 43:08-35, 45:03-18.

otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search" where the technology is not in general public use (internal quotations and citations omitted)). Defendants instead argue that the Pen Register Order satisfied the warrant requirement and that any intrusions on third parties' privacy interests are irrelevant to Andrews.

After his arrest, Andrews prevailed in state court on a motion to suppress contraband obtained as a result of the Hailstorm search. *State v. Andrews*, 134 A.3d 324, 354-56 (Md. Ct. Spec. App. 2016). The state court found that the Pen Register Order's vague disclosure of a far-reaching new search technology failed to meet the probable cause and particularity prongs of the warrant requirement. *Id.* at 360-61. Andrews then filed the present § 1983 suit against Defendants asserting, *inter alia*, a warrantless search in violation of the Fourth Amendment. The federal district court found that the Pen Register Order constituted a warrant authorizing use of a Hailstorm simulator. *Andrews v. Baltimore City Police Dep't*, Civil No. CCB-16-2010, 2018 WL 3649602, at *10 (D. Md. Aug. 1, 2018).

The district court declined to conduct factfinding into (1) the surveillance capabilities and configuration of the Hailstorm simulator and (2) the circumstances surrounding issuance of the Pen Register Order. Instead, the district court, after finding that "the [Pen Register Order] objectively authorized the use of a cell-site simulator," granted Defendants' motions for summary judgment. *Id.* at *9 n.9, *10. Andrews appealed.

The problem we face in resolving this appeal is that the record inadequately describes the degree of intrusion onto constitutionally protected areas that occurred as a result of the Hailstorm simulator's use. Defendants rely on limited testimony from a BPD

officer as to how he understood and operated the device, as well as public domain references describing cell site simulators generally. These sources tell us relatively little about what information the device gathered, and from whom.

For instance, although we know that the Hailstorm simulator forced an identification signal from every cellular device in its as-yet-unspecified operational range, we lack further detail on how many devices were identified. Moreover, the simulator's information collection capabilities may extend even further. *See* Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J.L. & Tech. 1, 11-12 (2014) (noting that cell site simulators can "intercept outgoing calls and text messages" by sending "signals, often indiscriminately, through the walls of homes, vehicles, purses, and pockets" (footnotes omitted)); *see also Patrick*, 842 F.3d at 547 (Wood, C.J., dissenting) (noting that "[b]ecause many third-party apps automatically send and receive data through the [cell phone] subscriber's network, it is reasonable to assume that a [cell site simulator] can collect other information from a cell phone, as well").

The Supreme Court has long directed us to consider, in evaluating an order purportedly authorizing a method of technological search, the degree of intrusion on individual privacy. *See Berger v. New York*, 388 U.S. 41, 59 (1967) (rejecting an order authorizing the use of an eavesdropping device in part because "the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation"); *see also Katz*

v. United States, 389 U.S. 347, 355-56 (1967) (in evaluating a warrant, courts must ensure "no greater invasion of privacy [i]s permitted than [i]s necessary under the circumstances . . . by authorizing the carefully limited use of electronic surveillance" (internal quotations omitted)); *United States v. Bobo*, 477 F.2d 974, 979 (4th Cir. 1973) ("[E]lectronic surveillance is permissible when judicially authorized under the most precise and discriminating circumstances which meet the requirements of the Fourth Amendment."). This determination ensures that execution of such an order "will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit" by enacting the Fourth Amendment, *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *see id.* at 84 n.8 (collecting cases), and "place[s] obstacles in the way of a too permeating police surveillance," *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

More recently, the Supreme Court has directed us to take special care in evaluating the reach of new technologies into protected areas. *See Carpenter*, 138 S. Ct. at 2223 ("[T]he Court is obligated—as 'subtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections." (alterations omitted) (quoting *Olmstead v. United States*, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting))); *see also Riley v. California*, 573 U.S. 373, 386, 393, 395 (2014) (noting that searches of cell phones "bear[] little resemblance" to traditional searches because "[c]ell phones differ in both a quantitative and a qualitative sense" due to their ability to store "a digital record of nearly every aspect of [a person's] li[fe]—from the mundane to the intimate"); *United States v.*

Jones, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring) (urging judicial caution where a new method of monitoring "is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously" because such a method "evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" (quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004))).

Absent a more detailed understanding of the Hailstorm simulator's configuration and surveillance capabilities, we cannot address the issues necessary for resolution of this case. Despite the government's use of a sophisticated, wide-reaching, and hard-to-detect new surveillance tool—one with potentially significant implications for constitutional privacy—we know very little about how many searches it conducted, of whom, and what data it collected and stored. We thus cannot strike the appropriate "balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers" that is central to the Fourth Amendment analysis. *Pennsylvania v. Mimms*, 434 U.S. 106, 109 (1977) (internal quotations omitted). We therefore remand this matter so that the district court may resolve certain factual issues and, if necessary, provide updated conclusions of law as to whether the Hailstorm simulator's use was a constitutional violation. Specifically, on remand, the district court is directed to conduct factfinding into the following characteristics of the Hailstorm cell site simulator:

(1) The maximum range at which the Hailstorm simulator can force nearby cellular devices to connect to it.

(2) The maximum number of cellular devices from which the Hailstorm simulator can force a connection.

(3) All categories of data the Hailstorm simulator may collect from a cellular device, regardless of whether such data is displayed to the Hailstorm simulator's operator in the course of locating a target phone, including by way of example and without limitation: cellular device identifiers (such as international mobile equipment identity ("IMEI") numbers, international mobile subscriber identity ("IMSI") numbers, and electronic serial numbers ("ESN")); metadata about cellular device operations (such as numbers dialed or texted, or webpages visited); and, most especially, the content of voice or video calls, text messages, emails, and application data.

(4) What data in (3) may be stored by the Hailstorm simulator.

(5) What data in (4) are accessible by law enforcement officers.

(6) All means by which the Hailstorm simulator was configured to minimize data collection from third party cellular devices not belonging to Andrews.

Furthermore, on remand, the district court should make 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 Pen Register Order, 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.

Following remand, the record as supplemented should underlie any updated conclusions of law as to whether or not BPD's use of the Hailstorm simulator constituted

a Fourth Amendment violation. We do not purport to direct the district court how to rule here, nor do we pass judgment on the result it has reached. We note only that, at this stage, more information is needed before an informed weighing of the interests may take place. Accordingly, we remand the case to the district court for further proceedings in accordance with this opinion. We will retain jurisdiction during the pendency of the remand proceedings.

REMANDED WITH INSTRUCTIONS

WILKINSON, Circuit Judge, concurring:

I am pleased to concur in the majority's opinion because it recognizes that the purpose of the remand is to develop the record and because it expressly declines to direct any particular result.

The majority rightly indicates that, in assessing the constitutionality of a search, the key concept is one of balance. Maj. Op. at 7. Of course, the balance between public safety and individual privacy is not easy to strike, for it is subject to the Fourth Amendment's broad command of reasonableness. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). But a balance must be struck. That being so, I do not understand the majority opinion to preclude the district court from taking cognizance as one side of that balance of the simulator's utility in ferreting out criminal offenses.

New surveillance technologies do carry the potential for increased invasions of privacy, but they also hold forth the promise of combatting serious crimes. *See United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 312 (1972). So much is apparent from this case. Using the Hailstorm simulator, officers were able to track down and apprehend Andrews, who had been eluding an arrest warrant for attempted murder. Where, as here, both significant governmental interests and significant privacy interests may well be at stake, the district court may find it profitable to inquire whether the important public interest in crime prevention and detection could have been served by means that were less intrusive and damaging to the "legitimate expectations of privacy" that citizens hold. *See Maryland v. King*, 569 U.S. 435, 461-62 (2013). Tailoring means

and ends is not unknown to the law, and it would seem to have special applicability as technology proceeds apace.