DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA
FOURTH DISTRICT

STATE OF FLORIDA,
Appellant,

v.

QUINTON REDELL SYLVESTRE,
Appellee.

No. 4D17-2116

[September 5, 2018]

Appeal and cross-appeal of non-final order from the Circuit Court for the Fifteenth Judicial Circuit, Palm Beach County; Samantha Schosberg Feuer, Judge; L.T. Case No. 502013CF003226BMB.

Pamela Jo Bondi, Attorney General, Tallahassee, and Melynda L. Melear, Senior Assistant Attorney General, West Palm Beach, for appellant.

Peter Grable, Palm Beach Gardens, for appellee.

KUNTZ, J.

The State applied for a search warrant based on information obtained from historical cell-site location information ("CSLI") and a cell-site simulator. After the Defendant moved to suppress evidence found during the search, the circuit court found probable cause existed to support the CSLI order. But the court suppressed evidence discovered through the State's warrantless use of the cell-site simulator.

The State appeals the court's order suppressing the search, and the Defendant cross-appeals the court's finding that the CSLI order was supported by probable cause. We affirm.

Background

The State charged the Defendant and two co-defendants with first-degree murder with a firearm while wearing a mask and six counts of robbery with a firearm while wearing a mask, arising from the robbery of a Boca Raton restaurant.

As part of its investigation, the State sought an order requiring the Defendant's cell phone service provider to disclose real-time CSLI for what it believed was the Defendant's cell phone number. A judge signed the "CSLI Order," which required the service provider to disclose "all cell-site activations and sectors for all incoming and outgoing calls/communications . . . call detail location records, 'angle from the tower' data, including contemporaneous (real-time) with these communications, and historical calls/communications detail records."

The judge also signed an order requiring the service provider to install a pen register and trap and trace device on the Defendant's phone and transmit the information collected to the Broward Sheriff's Office (the "Trap and Trace Order").

Later, the State applied for a search warrant of a Fort Lauderdale residence. The affidavit filed in support of the warrant stated that "[m]obile tracking was activated on [the Defendant's] cell phone pursuant to a lawful court order" and that the Defendant's phone was "placed specifically" at the residence and had been "stationary overnight within this residence for several concurrent nights." The search warrant was granted.

Detectives searched the residence and found a black backpack containing three firearms, a mask, ammunition, and a stun gun. The State tracked the location of the Defendant's cell phone and arrested him while he was driving into Palm Beach County.

After the Defendant's arrest, he moved to suppress all evidence recovered from the search of the residence. He argued that the CSLI Order was unsupported by probable cause, as required by *Tracey v. State*, 152 So. 3d 504 (Fla. 2014). He also argued that the State exceeded the scope of the CSLI Order by using a "cell-site simulator" to pinpoint his cell phone inside the residence.

At an evidentiary hearing, the court admitted transcripts of depositions, including that of a Broward Sheriff's Office sergeant. A defense witness described by the circuit court as a telecommunications expert also testified.

The sergeant testified that "at the time" the service provider "didn't provide GPS location information. It only provided tower information." With that information, the State located the cell phone to within only a general area, which the sergeant agreed could encompass several square

blocks. So he pinpointed the Defendant's phone at the residence "with the use of a cell-site simulator."

Similarly, the Defendant's expert testified that "there is not a technical capability in a pen register to give you a specific location, only the connection, which cell tower to which you were connected." In the words of the circuit court, the expert explained "that, at best, the CSLI Order could provide general location information, which would only be accurate for several square blocks of a particular area." Only a cell-site simulator could provide the State the exact location of the Defendant's cell phone.[1]

The court found that the CSLI Order was supported by probable cause. But it suppressed evidence obtained as a result of the warrantless use of the cell-site simulator. The State appealed the court's order suppressing the search of the residence. In a cross-appeal, the Defendant challenges the court's conclusion that the CSLI Order was supported by probable cause.

The Defendant's Cross-Appeal

We first address the Defendant's cross-appeal. Generally, in a criminal case, we lack jurisdiction to consider a defendant's appeal of a non-final order. But we do have jurisdiction to consider a defendant's cross-appeal when the issue relates to the issue raised in the state's appeal. *See* Fla. R. App. P. 9.140(b)(4) (2017). Thus, here, we have jurisdiction.

The Defendant argues that the CSLI Order was unsupported by probable cause because the affidavit did not establish that the cell phone's location would lead to evidence related to the restaurant robbery. He also argues that the statutes the State relied on when applying for the order do not require probable cause. *See* §§ 934.23, .42, Fla. Stat. (2012).

We affirm the circuit court's ruling that the CSLI Order was supported by probable cause. In the application for the order, the detective alleged that the Defendant was one of three men in surveillance video footage from the robbery. The application also alleged that a watch dealer identified the Defendant as the seller of a ladies' watch taken during the robbery. These facts, and others, were enough to establish probable cause.

---

[1] While the carousel of technological progress continues to move forward, the testimony presented to the circuit court does not. We recognize the ability to track a specific cell phone to a precise location continues to improve. But the Sergeant and the Defendant's expert testified in 2016 and 2017 about a search that took place in 2013, and we state the facts as presented to the circuit court.

We also address the Defendant's argument that the CSLI Order is insufficient because it was not a warrant. Relying on section 934.42, Florida Statutes (2012), the Defendant argues that "not only does subsection (4) not require a probable cause determination by the Magistrate, but specifically states that it may not require 'greater specificity or additional information beyond which is required by this section.'" So, according to the Defendant, the circuit court could not find probable cause in support of the CSLI Order because the statute authorizing the CSLI Order does not require probable cause. "By strict statutory construction," he argues, "everything contained in the fact section [of the affidavit] was superfluous."

We agree that the statute prevents a court from imposing a stricter standard when reviewing an application for a CSLI Order. But the statute does not prevent a court from making additional findings to support a showing of probable cause. Had the court not made those findings, the CSLI Order would have violated the Fourth Amendment. *See Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018); *Tracey*, 152 So. 3d at 525. Thus, the court's additional findings were not "superfluous," but necessary.

The content of a court's order—not the label affixed to it—determines whether a warrant satisfies the Fourth Amendment. Here, in issuing the CSLI Order, the court found probable cause existed. We affirm.

The State's Appeal

The State argues the court erred in suppressing the search of the residence because (1) the CSLI Order permitted the use of a cell-site simulator, and (2) the State did not have to disclose its intention to use a cell-site simulator.

i. Cell-Site Simulators

"A cell-site simulator—sometimes referred to as a 'StingRay,' 'Hailstorm,' or 'TriggerFish'—is a device that locates cell phones by mimicking the service provider's cell tower (or 'cell-site') and forcing cell phones to transmit 'pings' to the simulator." *United States v. Lambis*, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016).

At the evidentiary hearing, the Defendant's expert read from a House Committee Report and a Department of Justice Policy Guidance document to explain cell-site simulators. Those documents explain that "[l]aw

enforcement agents can use cell-site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator user's vicinity." U.S. DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 1 (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download.

Generally, a cell-site simulator "transform[s] a cell phone into a real time tracking device." Staff of Comm. on the Oversight and Government Reform, 114th Cong., *Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations* (Dec. 19, 2016), https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf. It "'tricks' nearby cell phones into thinking that it's a cell tower, thereby causing nearby cell phones to send signals to the device, which allows the operator of the device to locate the phone being sought." *United States v. Artis*, No. 16-CR-00477-VC, 2018 WL 3241400, at *2 (N.D. Cal. July 3, 2018) (citations omitted); *see also Lambis*, 197 F. Supp. 3d at 609.

Thus, cell-site simulators present significant privacy concerns. At the same time, they "are invaluable law enforcement tools that locate or identify mobile devices during active criminal investigations." U.S. DEP'T OF HOMELAND SECURITY, DEPARTMENT POLICY REGARDING THE USE OF CELL-SITE SIMULATOR TECHNOLOGY 1 (Oct. 19, 2015), https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf.

These competing interests are not novel. Technological advancement often collides with the Fourth Amendment. When balancing these interests, we must "ensure that the 'progress of science' does not erode Fourth Amendment protections." *Carpenter*, 138 S. Ct. at 2223 (quoting *Olmstead v. United States*, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting)). To do so, the Supreme Court appears to "adjust[] legal rules to restore the preexisting balance of police power" as technology advances. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 482 (2011).

For example, in *Katz* the Supreme Court held that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz v. United States*, 389 U.S. 347, 351–52 (1967). The "Court suggested for the first time that a search triggering the Fourth Amendment occurs when the government violates an 'expectation of privacy' that 'society is prepared to recognize as reasonable.'" *Carpenter*,

138 S. Ct. at 2261 (Gorsuch, J., dissenting) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

After *Katz*, the Supreme Court rejected the government's "contention that it should be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime is being or will be committed and that monitoring the beeper wherever it goes is likely to produce evidence of criminal activity." *United States v. Karo*, 468 U.S. 705, 717 (1984). The Supreme Court found "[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight." *Id.* at 716 (footnote omitted).

Later, the Supreme Court held that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

More recently, the Supreme Court held that attaching a GPS tracking device to a vehicle constitutes a search under the Fourth Amendment. *United States v. Jones*, 565 U.S. 400, 404 (2012). Two years later, the Supreme Court held that "a warrant is generally required before such a search [of a cell phone], even when a cell phone is seized incident to arrest." *Riley v. California*, 134 S. Ct. 2473, 2493 (2014). The Court recognized that cell phones hold "the privacies of life," *id.* at 2495 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)), and noted that "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.*

Following *Riley*, the Florida Supreme Court held that a defendant

> had a subjective expectation of privacy in the location signals transmitted solely to enable the private and personal use of his cell phone, even on public roads, and that he did not voluntarily convey that information to the service provider for any purpose other than for its intended purpose.

Tracey, 152 So. 3d at 525.

And recently, the United States Supreme Court recognized the "deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach,

and the inescapable and automatic nature of its collection[.]" *Carpenter*, 138 S. Ct. at 2223. The Supreme Court stated:

> [T]he 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, "after consulting the lessons of history," drafted the Fourth Amendment to prevent.

Id. (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). Thus, the Supreme Court applied Professor Kerr's equilibrium-adjustment theory and held that the government "must generally obtain a warrant supported by probable cause before acquiring such records." *Id.* at 2221.

Together these cases hold that, without a warrant, the government cannot: use technology to view information not visible to the naked eye, attach a device to property to monitor your location, search a cell phone in your possession without a warrant, or obtain real-time location information from the cell carrier.

With a cell-site simulator, the government does more than obtain data held by a third party. The government surreptitiously intercepts a signal that the user intended to send to a carrier's cell-site tower or independently pings a cell phone to determine its location. Not only that, a cell-site simulator also intercepts the data of other cell phones in the area, including the phones of people not being investigated.

If a warrant is required for the government to obtain historical cell-site information voluntarily maintained and in the possession of a third party, *see Carpenter*, 138 S. Ct. at 2221, we can discern no reason why a warrant would not be required for the more invasive use of a cell-site simulator. *See, e.g.*, *United States v. Ellis*, 270 F. Supp. 3d 1134, 1145 (N.D. Cal. 2017). This is especially true when the cell phone is in a private residence, *Karo*, 468 U.S. at 718, or other private locations "beyond public thoroughfares" including "doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter*, 138 S. Ct. at 2218.

Thus, absent a valid exception to the warrant requirement, the government must establish probable cause and receive court authorization before using a cell-site simulator. In other words, "get a warrant." *Riley*, 134 S. Ct. at 2495.

ii. The Evidence Obtained As a Result of the Warrantless Use of a Cell-Site Simulator

The State "acknowledges that cell phones are 'effects' under the Fourth Amendment, and that a person has a subjective expectation of privacy in the location signals emitted from his or her cell phone." It argues the CSLI Order and the simultaneously issued Trap and Trace Order satisfied the warrant requirement. Those orders did not authorize the use of a cell-site simulator.

A pen register and trap and trace device, according to the Defendant's expert, has a specific, but limited, use. *See Smith v. Maryland*, 442 U.S. 735, 741 (1979). The Trap and Trace Order here did not include a finding of probable cause and did not authorize location tracking.

The CSLI Order authorized the acquisition of location information. But it was directed to records "monitored and maintained by the provider," and included location data "received by said electronic communication provider" or "available from the said electronic communication provider." It required the "electronic communication provider" to "disclose" the data or make it available "through reasonable means."

The CSLI Order required the service provider to disclose information in its possession to the Broward Sherriff's Office. It did not authorize action by the State. Thus, the CSLI Order did not permit the use of a cell-site simulator. *Lambis*, 197 F. Supp. 3d at 611 ("The fact that the DEA had obtained a warrant for CSLI from the target cell phone does not change the equation."); *see also People v. Smith*, No. 1–14–1814, 2017 WL 6722818, at *18 (Ill. App. Ct. Dec. 27, 2017); *People v. Gordon*, 68 N.Y.S.3d 306, 311 (N.Y. Sup. Ct. 2017); *State v. Andrews*, 134 A.3d 324, 327 (Md. Ct. Spec. App. 2016).

The CSLI Order did not authorize the State to act independently. But the sergeant and the Defendant's expert testified that the information maintained by the service provider could not identify the exact location of the Defendant's phone. So the State resorted to other means.

In other words, the CSLI Order authorized *indirect* government surveillance. But the State could not obtain the information it required through the authorized means. So the State conducted *direct* government surveillance by using a cell-site simulator. And it did so without a warrant. Based on controlling Supreme Court authority, the court correctly suppressed the evidence obtained as a result of the State's warrantless actions.

Conclusion

We affirm the order finding probable cause existed for issuing the CSLI Order, but suppressing evidence discovered as a result of the State's use of a cell-site simulator.

Affirmed.

WARNER and DAMOORGIAN, JJ., concur.

* * *

Not final until disposition of timely filed motion for rehearing.