**NOT FOR PUBLICATION WITHOUT THE APPROVAL OF THE APPELLATE DIVISION**

This opinion shall not "constitute precedent or be binding upon any court." Although it is posted on the internet, this opinion is binding only on the parties in the case and its use in other cases is limited. R. 1:36-3.

SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-2010-24

STATE OF NEW JERSEY,

Plaintiff-Respondent,

v.

MICHAEL A. HOBBS,

Defendant-Appellant.

---

Argued September 17, 2026 – Decided October 2, 2026

Before Judges Mawla, DeAlmeida, and Chase.

On appeal from the Superior Court of New Jersey, Law Division, Morris County, Indictment No. 22-06-0423.

Margaret McLane, Assistant Deputy Public Defender, argued the cause for appellant (Jennifer N. Sellitti, Public Defender, attorney; Margaret McLane, of counsel and on the briefs).

Bethany L. Deal, Deputy Attorney General, argued the cause for respondent (Jennifer Davenport, Attorney General, attorney; Bethany L. Deal, of counsel and on the brief).

PER CURIAM

After the Law Division denied his motion to suppress evidence obtained through geofence warrants—warrants that require cell phone service providers to produce location data for users in a specific location during a specific time—defendant Michael Hobbs pleaded guilty to three counts of first-degree robbery, N.J.S.A. 2C:15-1(a)(1), and the court sentenced him to an eleven-year prison term subject to the No Early Release Act, N.J.S.A. 2C:43-7.2. He now appeals from the order denying suppression and raises the following arguments:

> POINT I
>
> THE SEARCH OF MILLIONS OF USERS' LOCATION INFORMATION AND THE WARRANTLESS IDENTIFICATION OF DEFENDANT'S SUBSCRIBER INFORMATION WERE UNCONSTITUTIONAL.
>
> > A. There Was No Probable Cause To Believe That Evidence Of Criminal Activity Would Be Discovered Through The Warrants.
> >
> > B. The Warrants Were Overbroad And Lacked Particularity Because They Allowed For The Return Of Location Information Of Users Who Were Outside Of The Geofence.
> >
> > C. The Warrants Impermissibly Allowed Police To Get Whatever Deanonymized Subscriber Information They Deemed Relevant.

D. Geofence Warrants Are Always Unconstitutional General Warrants.

After reviewing the record and the parties' arguments, we reverse and remand.

I.

Between January 21 and January 26, 2022, six armed robberies occurred at gas stations in Morris and Warren counties. The robberies shared a similar modus operandi. Detective Matthew G. Belcastro of the Morris County Prosecutor's Office summarized the relevant facts in his probable cause affidavit.

On January 21, at about 7:54 p.m., a man robbed a Shell gas station in Morris County. Witnesses described him as a Black male driving a black BMW X6 and wearing black clothing, including a black face covering. After asking the attendant for fuel, he brandished a knife, demanded cash, took about $100, and fled.

About ten minutes later, at approximately 8:04 p.m., a man robbed a Conoco gas station in Morris County. Witnesses again described him as a Black male driving a black BMW X6 SUV and wearing black clothing, including a black hat. He asked for fuel, exited the vehicle, brandished a knife, demanded cash, took about $700, pushed the attendant to the ground, and fled.

Three days later, at about 11:39 p.m., two men robbed an Exxon gas station in Morris County. Witnesses described both men as Black males traveling in a black BMW X6 SUV. The passenger, who wore dark clothing and tan boots, exited the vehicle, brandished an older-style metal handgun, demanded cash, and fled with the driver after they took about $400.

Approximately thirty-five minutes later, a Morris County Fuel 4 gas station was robbed by "a black male driver and a black male passenger" operating a black BMW X6 SUV. The passenger, wearing all dark clothing and tan boots, exited the vehicle after the driver requested fuel from the attendant. Then, the passenger brandished a handgun, stole between $200 and $300, and fled. Surveillance video showed the BMW displayed temporary New Jersey tags, "X01691." Investigators later learned the tags were stolen in Orange Township.

On January 26, at about 10:56 p.m., two men robbed a QuickChek gas station in Warren County. Witnesses described the driver and passenger as Black males traveling in a black BMW X6 SUV. The driver was described as wearing dark clothing and a dark hat. He asked the attendant for fuel, and once the vehicle was full, the passenger brandished a black handgun, and both men demanded cash. After taking approximately $537 in cash both suspects fled.

Surveillance video indicated the BMW bore New Jersey license plate, "U88DUH." Subsequent investigation determined the plate was stolen in Newark.

Later that night, two men robbed a Shell gas station in Morris County. Witnesses described the driver and passenger as Black males traveling in a black BMW X6 SUV. The passenger, dressed in dark clothing and a black face covering, exited the vehicle, brandished a black semiautomatic handgun, demanded cash, took approximately $208, and fled with the driver.

As part of his investigation, Detective Belcastro applied to the court for a Communications Data Warrant directed to Google. The warrant sought geofence data.

Google offers a service called Google Location History (LH). For users who opt in, by using their cell phone, LH stores records of their whereabouts over time. In effect, LH creates a virtual journal of a user's movements. Users who opt in receive benefits such as personalized maps, recommendations, real-time traffic updates, and help locating lost devices. LH is not only created, edited, and stored for the benefit of users who opt into the service, it also reveals a user's location and movements with a much higher degree of precision than cell site location information (CSLI). To use Google's LH service, a person

must: (1) own a smartphone; (2) turn on the device's location setting; (3) allow applications to use location information; (4) opt in to LH and location reporting in the device's settings; and (5) sign in to a Google account on the device and carry it while traveling.

Once a user takes those steps, their location data is stored on Google's cloud-based servers. Here, the parties refer to Google's cloud-based storage server as "Sensorvault."[1] Although Google stores the information, the user controls it and may edit or delete it, in whole or in part. The user's control over this data further distinguishes LH from CSLI—which wireless carriers collect and maintain for business purposes.

Typically, law enforcement identifies a point of interest—usually a crime scene—and seeks LH data for users within a certain radius of that point at about the time of the crime. A geofence warrant therefore compels Google to produce this data from its LH service.

Google generally responds to geofence warrants in three steps. First, it searches Sensorvault to identify users with potentially responsive LH data. It then compares that data to the warrant's time-and-place limits and produces an

[1] Google has changed its method for storing user location data. It is now stored on an individual's phone rather than in Sensorvault on Google's servers.

anonymized list of responsive devices. That list includes an anonymized device number, coordinates, a timestamp, a radius, and an indicator showing whether the data came from Wi-Fi, GPS, or a cell tower. Second, law enforcement reviews the anonymized data and identifies devices of interest. At that stage, officers may ask Google for additional contextual coordinates to help eliminate false positives. Third, law enforcement selects the devices for which it seeks identifying account information, and Google then provides that information, often including a Gmail address and the account holder's name.

Detective Belcastro's affidavit stated Google's LH data could "assist investigators in forming a fuller geospatial understanding and timeline related to a specific criminal investigation; and may tend to identify potential witnesses and/or suspects." He further certified:

> there is probable cause to believe that information stored on the [p]roviders' servers associated with the Google accounts and/or devices located at the location and timeframe specified, will contain evidence, fruits, and instrumentalities of the subject offense, and therefore there is probable cause for this court to issue said CDW/[s]earch [w]arrant to Google to provide the information associated with the places described . . . .

On January 28, 2022, a Superior Court Judge approved the warrant sought by Detective Belcastro. The warrant: (1) authorized law enforcement to obtain LH data associated with devices that were in or around the individual gas

stations during the timeframe the robberies occurred;[2] (2) outlined that Google was to send anonymized data and that law enforcement would review the data to determine which users "were in more than one" of the identified areas or which users' movement patterns were "consistent with the crime"; (3) permitted law enforcement to request identifying account information based on their determinations; and (4) required that Google identify the requested users and provide, to the extent available, the users' name, subscriber information, date of birth, account type and number, email(s), devices associated with the account, and telephone number.

Google responded to the warrant and provided a single anonymous user identification number. However, it produced data for only three of the six requested locations because of errors in the geographic formatting.

Detective Belcastro then applied for a second geofence warrant seeking LH data for the three locations for which Google was unable to provide. A second judge granted that warrant with the same stipulations as the previous search warrant. Google responded to the second geofence warrant and provided ninety-five anonymous account numbers. After reviewing the data and cross-referencing across each location, Detective Belcastro ascertained that one

[2] The "timeframe" was a thirty-minute window.

anonymous user "was reported across all three locations." Accordingly, he requested Google deanonymize that account—which was found to belong to defendant.

On July 6, 2022, a Morris County grand jury returned a fourteen count indictment charging defendant with: five counts of first-degree robbery, N.J.S.A. 2C:15-1(a)(1), (2), (counts one, four, seven, eight, and ten); three counts of third-degree possession of a weapon for an unlawful purpose, N.J.S.A. 2C:39-4(d), (counts two, five, and eleven); three counts of fourth-degree unlawful possession of a weapon, N.J.S.A. 2C:39-5(d), (counts three, six, and twelve); second-degree conspiracy to commit robbery, N.J.S.A. 2C:5-2, (count nine); second-degree eluding, N.J.S.A. 2C:29-2(b), (count thirteen); and third-degree receiving stolen property, N.J.S.A. 2C:20-7(a), (count fourteen).

Defendant moved to suppress, arguing the warrant lacked probable cause and particularity and further, that geofence warrants are unconstitutional general warrants. At oral argument, the court noted the "Fourth Amendment does not deal in precision, but, rather, probability[,]" and "the State ha[d] structured the geofence zones to minimize the potential for capturing location data for uninvolved individuals and maximize the potential for capturing the location data for suspects and witnesses."

As to probable cause, the court stated "[t]here is also probable cause that evidence of the crime will be located at Google because the location data on cell phones at the scene of the robbery certainly can provide evidence on the identity of the perpetrators and the witnesses to the crime." Although acknowledging the warrant applications did not proffer evidence of cell phone use, the court concluded, given the "ubiquity of cell[ ]phones and their common usage" coupled with the Bluetooth and GPS capabilities of the vehicle used, it was reasonable to infer—especially given Detective Belcastro's training and experience—"that the suspects conducting multiple robberies across the State, as well as any possible passerby witnesses[,] would have had cell[ ]phones."

The court found the warrant "did particularly describe the places to be searched because it narrowly identified the target areas of the geofence data by time and location and [was] not overbroad in scope." The timeframes for which LH data was sought were "narrowly configured to capture specific time periods reasonably expected to correlate with evidence of the gas station robberies."

Moreover, the court found the warrants were adequately specific, given they were limited "to the timeframe of the robbery incidents[,]" and "narrowly crafted to ensure that the location data with fair probability will capture evidence of the crime only." Defendant's motion to suppress was denied on December 5,

2024. His guilty plea and sentencing followed in January and February 2025, respectively.

II.

The scope of our review regarding a motion to suppress is limited. State v. Ahmad, 246 N.J. 592, 609 (2021); see also State v. Nelson, 237 N.J. 540, 551 (2019). The motion court's factual determinations "must be upheld when '. . . supported by sufficient credible evidence in the record.'" State v. A.M., 237 N.J. 384, 395 (2019) (quoting State v. S.S., 229 N.J. 360, 374 (2017)). However, we owe no deference to the trial court's legal conclusions or interpretation of the legal consequences that flow from established facts. State v. Gamble, 218 N.J. 412, 425 (2014). Our review in that regard is de novo. State v. Watts, 223 N.J. 503, 516 (2015).

III.

The Fourth Amendment of the United States Constitution and Article I, Paragraph 7 of the New Jersey Constitution protect citizens from unreasonable searches and seizures. To conduct a search, police ordinarily must obtain a warrant from a neutral judicial officer. U.S. Const. amend. IV; N.J. Const. art. I, ¶ 7. In warrant applications, police must describe the places they want to search, the people or things they intend to seize with particularity, and explain

what probable cause exists to believe evidence of a crime will be found at the place being searched. R. 3:5-3(b); State v. Jones, 179 N.J. 377, 388 (2004).

A search warrant enjoys a presumption of validity. State v. Bivins, 226 N.J. 1, 11 (2016). "[S]ubstantial deference must be paid by a reviewing court to the determination of the judge who has made a finding of probable cause to issue a search warrant." State v. Missak, 476 N.J. Super. 302, 317 (App. Div. 2023) (alteration in original) (quoting State v. Evers, 175 N.J. 355, 381 (2003)), leave to appeal granted, 263 N.J. 321 (2026). Any "[d]oubt as to the validity of the warrant 'should ordinarily be resolved by sustaining the search.'" State v. Keyes, 184 N.J. 541, 554 (2005) (quoting Jones, 179 N.J. at 389). We will reverse an order authorizing a search warrant that is "so clearly mistaken 'that the interests of justice demand intervention and correction.'" Gamble, 218 N.J. at 425 (quoting State v. Elders, 192 N.J. 224, 244 (2007)).

In State v. Earls, our Supreme Court held individuals have a constitutional privacy interest in cell-phone location information. 214 N.J. 564, 568 (2013). The Court noted:

> Using a cell phone to determine the location of its owner can be far more revealing than acquiring toll billing, bank, or Internet subscriber records. It is akin to using a tracking device and can function as a substitute for 24/7 surveillance without police having to confront the limits of their resources. It also involves

> a degree of intrusion that a reasonable person would not anticipate. . .Location information gleaned from a cell[ ]phone provider can reveal not just where people go—which doctors, religious services, and stores they visit—but also the people and groups they choose to affiliate with and when they actually do so. That information cuts across a broad range of personal ties with family, friends, political groups, health care providers, and others. In other words, details about the location of a cell phone can provide an intimate picture of one's daily life.
>
> [Id. at 586 (citations omitted).]

The Court also held

> cell phones are not meant to serve as tracking devices to locate their owners wherever they may be. People buy cell phones to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a cell phone to share detailed information about their whereabouts with the police.
>
> [Id. at 587.]

Thus, the Court concluded "police must obtain a warrant based on a showing of probable cause, or qualify for an exception to the warrant requirement, to obtain tracking information through the use of a cell phone." Id. at 588.

On June 29, 2026, the United States Supreme Court held geofence warrants are searches for Fourth Amendment purposes because individuals have a reasonable expectation of privacy in records of their cell-phone location. Chatrie v. United States, 609 U.S. ___ (2026) (slip op. at 2). The Court did not

resolve whether the warrant there was reasonable in all respects. Instead, it left to the lower courts whether each step of the search was described with sufficient particularity and supported by probable cause. Ibid.

The Court's holding that geofence warrants are Fourth Amendment searches was rooted in the premise that "the Fourth Amendment protects people, not places[,]" Katz v. United States, 389 U.S. 347, 351 (1967), and has been "expanded . . . to protect certain expectations of privacy as well." Carpenter v. United States, 585 U.S. 296, 304 (2018); see also Chatrie, 609 U.S. at ____ (slip op. at 11) (citing Soldal v. Cook Cnty., 506 U.S. 56, 64 (1992)). Although geofence warrants provide law enforcement with a much-needed technical apparatus to apprehend perpetrators who may otherwise evade justice, because of Earls and Chatrie, the use of a search warrant supported by probable cause is required.

A.

Defendant's principal argument on appeal is the State failed to establish probable cause to believe Google's servers contained evidence of the crimes. See State v. Marshall, 199 N.J. 602, 610 (2009) ("a warrant should not issue unless the court is satisfied that there is 'probable cause to believe . . . that evidence of a crime is at the place sought to be searched.'") (quoting State v.

Sullivan, 169 N.J. 204, 210 (2009)). He submits the trial court erred in relying on general propositions and the "ubiquity of [cell phones]" to support probable cause. Furthermore, Detective Belcastro's warrant application was devoid of any information alleging: (1) the perpetrator of the robberies was possessing a smartphone; (2) there was a Google account, with LH enabled, on the smartphone; and (3) the perpetrator of the robberies was logged into their Google account at the time of the crimes.

A defendant challenging the validity of a search warrant "has the burden to prove 'that there was no probable cause supporting the issuance of the warrant or that the search was otherwise unreasonable.'" Marshall, 199 N.J. at 612 (quoting Jones, 179 N.J. at 388 (quoting State v. Valencia, 93 N.J. 126, 133 (1983))). "Courts . . . should sustain the validity of a search only if the finding of probable cause relies on adequate facts." State v. Boone, 232 N.J. 417, 427 (2017) (citing Jones, 179 N.J. at 388-89). This is true even "[w]hen the adequacy of the facts offered to show probable cause . . . appears to be marginal." Missak, 476 N.J. Super. at 317 (quoting State v. Kasabucki, 52 N.J. 110, 116 (1968)).

Probable cause "eludes precise definition." State v. Gathers, 234 N.J. 208, 220 (2018) (quoting Keyes, 184 N.J. at 553). It is a "practical" and

"nontechnical" standard addressing "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." State v. Morgan, 479 N.J. Super. 420, 428 (App. Div. 2024) (quoting State v. Basil, 202 N.J. 570, 585 (2010)). It does not require "legal evidence necessary to convict." Gathers, 234 N.J. at 220. That said, it requires "more than a mere hunch or bare suspicion." Missak, 476 N.J. at 321 (quoting State v. Irelan, 375 N.J. Super. 100, 118 (App. Div. 2005)).

"[E]stablishing probable cause for a search requires more than a showing of what 'may' have occurred." Ibid. When courts grant a warrant, they are tasked with "'mak[ing] a practical, common sense determination whether, given all of the circumstances, there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" State v. O'Neal, 190 N.J. 601, 612 (2007) (quoting State v. Moore, 181 N.J. 40, 46 (2004)); see also State v. Johnson, 171 N.J. 192, 214 (2002) (citations omitted, punctuation in original).

The fact that cell phones are common, and many people always carry them, does not by itself establish probable cause to search Google's Sensorvault. If it did, police could seek geofence warrants in virtually every criminal investigation. That would drain the probable-cause requirement of meaning. Although probable cause is a low threshold, law enforcement cannot guess or

root their assertions in broad generalizations. See State ex rel. J.G., 151 N.J. 565, 591 (1997) (requiring "more than raw, unsupported suspicion").

Beyond the robbery facts themselves, the warrant affidavit offered little that tied the crimes to Google's records. Instead, it largely described how cell phones work, how Google stores LH data, and how that data might assist the investigation. The affidavit did not establish a nexus between the suspects and Google's servers. To bridge that gap, the issuing court had to assume defendant had a smartphone, carried it during the robberies, had a Google account, had opted in to LH and location reporting, had enabled the relevant location settings, had signed in to that Google account on the phone, and had done all of those things at the time of the robberies.

Maybe all those things happened, but "establishing probable cause for a search requires more than a showing of what 'may' have occurred," and assumptions, hunches, and "'bare suspicion'" are not enough to support a finding of probable cause. Missak, 476 N.J. Super. at 321 (quoting Irelan, 375 N.J. Super. at 118). As such, we are constrained to reverse the denial of the suppression motion.

The warrant affidavit could have strengthened the application in at least two ways. It could have included additional facts supporting an inference the

suspects used cell phones to communicate with each other during, or immediately preceding or following, the commission of the robberies. Or it could have explained, based on his training and experience, that multiple-suspect robberies of this kind typically involve cell phones for mapping purposes. Without these assertions, the warrant lacked sufficient probable cause to support the proposition that Google's Sensorvault contained evidence of the crimes. And, finally because the warrants were not supported by probable cause, we need not address defendant's remaining arguments.

Reversed and remanded for further proceedings. We do not retain jurisdiction.

I hereby certify that the foregoing is
a true copy of the original on file in
my office.
M.C. Hurley
Clerk of the Appellate Division