SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-3963-23

STATE OF NEW JERSEY,

Plaintiff-Appellant,

v.

VAN SALTER,

Defendant-Respondent.

———————————————

Argued December 16, 2024 – Decided May 20, 2025

Before Judges Gummer, Berdote Byrne,[1] and Jacobs (Judge Gummer dissenting).

On appeal from an interlocutory order of the Superior Court of New Jersey, Law Division, Middlesex County, Indictment Nos. 23-08-0913 and 23-08-0914.

Randolph E. Mershon III, Assistant Prosecutor, argued the cause for appellant (Yolanda Ciccone, Middlesex County Prosecutor, attorney; Randolph E. Mershon III, of counsel and on the brief).

[1] Judge Berdote Byrne was added to the panel after oral argument with the consent of all counsel.

Tamar Y. Lerer, Deputy Public Defender, argued the cause for respondent (Jennifer N. Sellitti, Public Defender, attorney; Tamar Y. Lerer, of counsel and on the briefs).

Jennifer Stisa Granick (American Civil Liberties Union Foundation) of the California bar, admitted pro hac vice, argued the cause for amici curiae American Civil Liberties Union, American Civil Liberties Union of New Jersey, Electronic Frontier Foundation, and National Association of Criminal Defense Lawyers (Jennifer Stisa Granick, and Nathan Freed Wessler (American Civil Liberties Union Foundation) of the New York and Commonwealth of Massachusetts bars, admitted pro hac vice, attorneys for amicus curiae American Civil Liberties Union; Jennifer Stisa Granick and Nathan Freed Wessler, on the joint brief).

American Civil Liberties Union of New Jersey Foundation, attorneys for amicus curiae American Civil Liberties Union, American Civil Liberties Union of New Jersey (Dillon Scott Reisman and Jeanne M. LoCicero, on the joint brief).

Pashman Stein Walder Hayden, attorneys for amicus curiae National Association of Criminal Defense Lawyers (Alan Silber, on the joint brief).

James E. Moore, Assistant Prosecutor, argued the cause for amicus curiae County Prosecutors Association of New Jersey (Mark Musella, Bergen County Prosecutor, attorney; James E. Moore, of counsel and on the brief).

PER CURIAM

In today's digital world, advances in technology have transformed cell phones from simple communication devices into personal computers. Cell

phones are now used for navigation, banking, shopping, traveling, exercising, photography, and storing personal information—the full gamut of daily activity. Mobile devices may be enabled to track locations, trace movements, identify consumer preferences, and monitor internet activities. As their functions have broadened, cellular service providers hold a cache of data that grows with every user interaction and has become a powerful tool not only in commerce but increasingly in criminal investigations.

Law enforcement considers this trove of information essential in identifying suspects and solving crimes. Anne Toomey McKenna & Clifford S. Fishman, Wiretapping and Eavesdropping § 29:38 (rev. Dec. 2024). Thus, the court is increasingly called upon to ensure law enforcement's use of technological advances does not unlawfully encroach upon an individual's constitutionally-mandated privacy protections.

We consider today a matter of first impression in New Jersey: whether geofence warrants, which focus on a particular location during a specific time period and require cellular service providers to search their proprietary databases to identify cell phones present at that location and time, amount to an unconstitutional invasion of privacy under the New Jersey Constitution. We conclude geofence warrants are not unconstitutional per se and instead require

a fact-specific inquiry into the probable cause supporting each warrant. We also find the first of three warrants issued in a sequential process was correctly issued based on probable cause and vacate the trial court's order granting defendant's motion to suppress. We remand for a fact-driven, probable cause analysis of the second and third warrants at issue in this case.

I.

On March 16, 2022, officers of the Milltown Police Department responded to a gas service station and spoke with a store employee located within the service station complex. She told officers that a male came into the store at 8:59 p.m. wearing a grey-hooded sweatshirt, winter gloves, a large black-and-white checkered scarf tied around his neck and shoulders, and a black facial mask. The employee heard the male speaking aloud to a non-present third-party. According to the employee, "it seemed like [he] was speaking to a female who was pregnant because he was stating something to the effect that it was not a good idea for her to smoke while she was pregnant." A female customer entered the store and also heard the male speaking. Because he was not speaking to her or to the employee, the customer believed the perpetrator was talking to someone as if he were on a phone.

The perpetrator purchased a number of items and handled others. After the customer left the store, the perpetrator came around the counter, pulled out a handgun, and held it to the employee's neck, demanding money from the registers. The employee handed over $673, after which the perpetrator led the employee to a back room where he punched her several times, threw her to the ground, and told her to lie down and count to ten. He then fled the store.

Also working at the service station was a gas pump attendant. From his vantage point outside of the store, the attendant witnessed the perpetrator go behind the counter and strike the employee. The attendant called police after he observed the perpetrator flee the store.

The police were unable to locate a suspect or surveillance cameras in the surrounding area. However, a surveillance camera at the gas station captured the incident on video. The video showed the perpetrator walking into the store at 8:59 p.m. and leaving at 9:13 p.m. No DNA, fingerprint, or other forensic evidence was recovered from which to identify a suspect.

Because the perpetrator remained unidentified but was heard purportedly speaking to a third party while in the store, the detective applied for a geofence warrant. In support of the warrant, the detective provided the following information regarding cell phones:

19. Your Affiant knows that most people in today's society possess a cellular telephone or mobile telephone, which is a handheld, wireless device primarily used for voice, text, and data communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called "cells" or "cell sites," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") or other technology for determining a more precise location of the device. I know that most people will carry them whenever they leave their place of residence.

He provided the following information regarding Google:

20. This applicant also knows that Google, Inc. is a company which, among other things, provides electronic communication services to subscribers, including email services. Google allows subscribers to obtain email accounts at the domain name gmail.com and/or google.com. Subscribers obtain an account by registering with Google. A subscriber using the Provider's services can access his or her email account from any computer/device connected to the Internet.

21. This applicant knows that Google has also developed a proprietary operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a

Google account when they first turn on a new Android device.

22. Based on this applicant's training and experience, this applicant knows that Google, Inc. collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled. The company uses this information for location-based advertising and location-based search results and stored such data in perpetuity unless it is manually deleted by the user. This location information is derived from GPS data, cell site/cell tower information, Bluetooth connections, and Wi-Fi access points.

23. This applicant knows that location data can 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. Such information can also aid investigators in possibly inculpating or exculpating persons of interest.

24. Additionally, location information can be digitally integrated into image, video, or other computer files associated with a Google account and can indicate the geographic location of the account[']s user at a particular date and time (e.g., digital cameras, including on cellular telephones, frequently store GPS coordinates indicating where a photo was taken in the "metadata" of an image file).

The detective ended his certification by asserting "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 offenses." He also stated:

> The information sought from Google, Inc. regarding the Subject Accounts will assist in identifying which cellular devices were near the location where the crime being investigated occurred during the time frame it is currently believed to have occurred. This information may assist law enforcement in determining which persons were present or involved with the subject offense under investigation.

The detective supplied to the court the geographic coordinates of the gas service station and the fourteen-minute time window corresponding to the crime as recorded by the store surveillance camera.

The Warrant Application Process

On March 31, 2022, a Superior Court judge authorized the warrant application ("Warrant I"), finding "the facts in the submitted [c]ertification show probable cause for believing that the requested records and data will yield relevant evidence." The judge entered an order laying out the three-step process for police to follow, essentially adopting Google's internal procedure for

responding to geofence warrants. We explain that procedure in detail below as Google's process is key to determining the issues before us.

In 2018, Google and the Computer Crime and Intellectual Property Section of the United States Department of Justice ("DOJ") developed an internal procedure for Google's response to a geofence warrant to "ensure privacy protections for Google users. Google instituted a policy of objecting to any warrant that failed to include deidentification and narrowing measures." United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022) (omission and alteration in original), aff'd, 107 F.4th 319 (4th Cir. 2024), aff'd en banc, ___ F.4th ___ (4th Cir. 2025).

Google location history is derived from "a service that Google account holders may choose to use to keep track of locations they have visited while in possession of their compatible mobile devices." United States v. Rhine, 652 F. Supp. 3d 38, 67 (D.D.C. 2023), vacated and remanded to dismiss as moot, No. 23-3168 (D.C. Cir. Feb. 3, 2025). Location history is determined based on "'multiple inputs,' including GPS signals, signals from nearby Wi-Fi networks, Bluetooth beacons, and cell towers." Ibid. "Location history even allows Google to estimat[e] . . . where a device is in terms of elevation." Chatrie, 590 F. Supp. 3d at 908 (alteration and omission in original) (internal quotation marks

omitted). Google stores this data in the "'Sensorvault' and associates each data point with a unique user account." Ibid. The Sensorvault "assigns each device a unique device ID - as opposed to a personal identifiable Google ID - and receives and stores all location history data in the Sensorvault to be used in ads marketing." Ibid. By default, location history is disabled as part of a device's factory setting. Ibid.; see also Rhine, 652 F. Supp. 3d at 67. "A user can initiate, or opt into, [l]ocation [h]istory either at the 'Settings' level, or when installing applications such as Google Assistant, Google Maps, or Google Photos." Chatrie, 590 F. Supp. 3d at 908. "Specifically, after logging into a Google account, a user must enable 'Location Reporting,' at which point [location history] data is sent to Google 'for processing and storage' in Google's 'Sensorvault.'" Rhine, 652 F. Supp. 3d at 67. Location history "logs a device's location, on average, every two minutes." Chatrie, 590 F. Supp. 3d at 908.

When seeking information pursuant to a geofence warrant from Google, law enforcement "(1) identifies a geographic area (also known as the 'geofence,' often a circle with a specified radius), (2) identifies a certain span of time, and (3) requests [l]ocation [h]istory data for all users who were within that area during that time." Id. at 914. "The requested time windows for these warrants might span a few minutes or a few hours." Ibid. (internal quotation marks

omitted). "In order to respond to a geofence warrant specifying a timeframe and location, Google has to compare all the data in the Sensorvault." Rhine, 652 F. Supp. 3d at 67 (emphasis omitted) (internal quotation marks omitted).

At Step 1, "Google must search . . . all [location history] data to identify users whose devices were present within the geofence during the defined timeframe." Chatrie, 590 F. Supp. 3d at 915 (omission and alteration in original) (emphasis omitted) (internal quotation marks omitted). "Google does not know which users may have . . . saved [location history] data before conducting th[is] search." Ibid. (omission and alterations in original). At Step 2, law enforcement "reviews the deidentified [data] to determine the [Sensorvault] device numbers of interest." Id. at 916 (alterations in original). "If law enforcement needs additional deidentified location information for a device to determine whether that device is actually relevant to the investigation, law enforcement, at this step, can compel Google to provide additional . . . location coordinates beyond the time and geographic scope of the original request." Ibid. (alterations and omission in original) (emphasis omitted) (internal quotation marks omitted).

"Finally, at Step 3, drawing from the de-identified data Google has produced so far, the [g]overnment can compel Google . . . to provide account-identifying information for the users the [g]overnment determines are relevant

to the investigation." Ibid. (omission in original) (emphasis omitted) (internal quotation marks omitted). "This account-identifying information includes the name and email address associated with the account." Ibid. (internal quotation marks omitted).

After it was served with Warrant I in this case, Google notified the police that a single cellular device had been logged into Google's location history during the specified time and within the given geographic boundaries. Because Google identified only one device in response to Warrant I, law enforcement did not need to employ Google's Step 2 to further winnow down the list. [2]

In June 2022, pursuant to Step 3, the detective applied for a warrant requiring production of "identifying account information" for that single device Google identified in response to Warrant I. In support of that application, the detective certified:

> 13. In a February 2018 study, Gartner (research company based in the United States) determined approximately 99.9% of all smartphones were either supported by Android OS or Apple iOS. Of

[2] We note a discrepancy in the respective certifications submitted as part of law enforcement's application for Warrants II and III: the certification in support of Warrant II provides Google's April 18, 2022 report identified only one device within the subject geographic search area. Further, the certification in support of Warrant III provides Google's April 18, 2022 report identified four devices within the subject geographic area, inclusive of the two employees, the witness, and defendant.

those, 86% were supported by Android OS and 14% were supported by Apple iOS.

14. [N]early every Android powered device has an associated Google, Inc. account. I also know that Apple iPhone's supports several Google, Inc. applications, such as Google Search, Gmail, Google Maps, and Google Drive, all of which require a Google, Inc. account. I also know Google, Inc. continuously tracks devices with an associated Google, Inc. account. I am also aware Android-based cellular phones report detailed location information to Google, where the geo-location and electronic data is then stored on their servers.

The detective explained, "[g]iven that almost all cellular phones and connected devices are either supported by Google, Inc. or support Google, Inc. software, and most people in today's society carry a cellular phone or other connected device on their person at nearly all times," he believed "it is likely the suspect(s) involved in this criminal investigation were in possession of at least one cellular phone/device, which was either powered by Android OS or had a cellular phone with a Google, Inc. application." The warrant application ("Warrant II") was authorized by a Superior Court judge. On receipt of Warrant II, Google identified defendant as the subscriber to whom the device was registered.

The detective then applied for a communications data warrant ("CDW" or "Warrant III") "to obtain from Google, Inc./Gmail Account the contents of stored electronic communications including all emails, . . . location information and full account information associated with" the now-identified suspect. The CDW was likewise authorized by a Superior Court judge.

Defendant's Arrest, Detention, and Motion to Suppress

Relying on the information obtained through the three warrants, law enforcement secured an arrest warrant and subsequently arrested defendant. The State moved to detain defendant without bail. That motion was granted. A Middlesex County grand jury returned an indictment charging defendant with first-degree robbery, N.J.S.A. 2C:15-1(a); second-degree possession of a firearm for an unlawful purpose, N.J.S.A. 2C:39-4(a)(1); second-degree aggravated assault, N.J.S.A. 2C:12-1(b)(1); fourth-degree aggravated assault, N.J.S.A. 2C:12-1(b)(4); and third-degree theft by unlawful taking, N.J.S.A. 2C:20-3(a). A second indictment against defendant was billed the same day charging him with first-degree unlawful possession of a handgun, N.J.S.A. 2C:39-5(b)(1) and 2C:39-5(j); and second-degree certain persons not to possess a firearm, N.J.S.A. 2C:39-7(b)(1).

Defendant moved to suppress all evidence seized pursuant to all three warrants based upon lack of probable cause. Defendant also moved to re-open his detention hearing; the court denied that motion in a February 29, 2024 order.

At the suppression hearing, counsel stipulated to the admission of exhibits into evidence including the authorized warrants, the detective's supporting certifications, and declarations filed in out-of-state cases; two of the declarations were submitted in Chatrie, and the third was submitted in People v. Dawes, No. 19002022 (Cal. Super. Ct. Sept. 30, 2022) from three Google employees describing the location information retrieval process. The motion court issued oral and written decisions, concluding the geofence search warrant (Warrant I) lacked probable cause and particularity.

In its oral ruling, the motion court referenced the witnesses who believed they had overheard defendant speaking via cell phone and found probable cause could not "be based on a hunch represented by a witness's claim that 'the subject was talking to someone as if he was on the phone . . . .'" The court continued:

> [T]o justify the search of a place, there must be a specific, objective, and particularized facts which, taken together, reasonably support the conclusion that evidence of the proceeds of criminal activity will be discovered in the place to be searched. In other words, there must be a nexus between the place to be searched and the evidence sought. At a minimum, this may require that a suspect be seen in possession of a cellular

> telephone within the area of a crime under investigation. As a preference, this should require that the geofence warrant list the identity of the person whose account is to be searched, which would include a particularized account of a physical cell phone with "location history" capability present within the geofence, because not all cellular telephones are smartphones capable of activating "location history" capability.
>
> In this case the account of the store clerk and the customer is not enough to support probable cause to believe a cell phone was at the scene. Neither witness saw the perpetrator with the cell phone. Both witnesses assumed the perpetrator had a cell phone because he is alleged to [have spoken] out loud to someone.
>
> To take it a step further, neither witness saw that the cell phone was a smartphone, if in fact there was a cell phone having a location history service feature activated. Assumptions like the ones made in this case cannot give rise to probable cause within the context of a geofence warrant application. Without more, they would likely fail as a basis for granting of any search warrant, given our case law.

Because the trial court rested its ruling on insufficiencies regarding the probable cause that defendant had used a cell phone while in the convenience store, it did not assess defense counsel's alternative arguments against the validity of any of the three search warrants.

After the court placed its suppression decision on the record, defendant again moved to re-open his detention hearing. The court granted defendant's

motion and ordered his release on Level 3+ monitoring in an August 8, 2024 order. On the State's application, we granted leave to appeal from the suppression order and stayed the release order pending appeal.

II.

Arguments on Appeal

On appeal, the State highlights that a search executed pursuant to a warrant is presumed valid, and, therefore, defendant bears the burden to prove there was no probable cause supporting the warrant. State v. Jones, 179 N.J. 377, 388 (2004). The State contends a "one-hundred percent certainty standard" is improper. Rather, the State maintains probable cause was properly found by the Superior Court judge who had authorized Warrant I based on a well-grounded suspicion that the suspect was using a cell phone, as two witnesses had overheard the suspect speaking to an unseen person about a subject not pertinent to the surrounding circumstances. Based on that information, a fair inference could be made the suspect was using a cell phone. Thus, the State contended, it was not sound for the court to rest "its entire probable cause determination on the fact that no one actually saw the cell phone to support the assertion that he was in possession of one."

The State also challenges the trial court's ruling "the warrant lacked particularity because it was not targeted to a particular individual or device," noting the trial court cited no case law holding a warrant invalid because it did not first "identify the person to be searched." The State maintains it did not have to particularly identify a defendant or his cell phone in its warrant application because "that was not the person, item or place that was being searched." Rather, the evidence sought was located on servers owned by Google and identified in the warrant application. Moreover, the State observes the warrant application precisely outlined the geographical and temporal parameters of the search to be conducted and, therefore, was sufficiently particularized.

The County Prosecutors Association of New Jersey, amicus to the State, maintains that geofence search warrants do not implicate the Fourth Amendment. It cites cases in which the Fourth and Eleventh Circuits rejected challenges to the constitutionality of geofence warrants, including Chatrie, and United States v. Davis, 109 F.4th 1320, 1328-29 (11th Cir. 2024).

The Association notes that unlike the cell phone user in our Supreme Court case of State v. Earls, 214 N.J. 564 (2013), whose location data was involuntarily provided by the user, the user here "absolutely [had] a choice to supply or refrain from supplying location data to Google" and that data "is not

essential to the operation of the device." Hence, according to the Association, this case "presents an entirely different technology that requires its own analysis." The Association asks this court to adopt the Fourth and Eleventh Circuits' approach.

Next, the Association observes geofence warrants seek limited, specific information, such as location "presence," within a geographical area and limited time period, not location "tracking." It merely provides the means to discover whether a certain device was present within a designated geofence. The Association also argues geofence warrants comply with the New Jersey Wiretapping and Electronic Surveillance Control Act, N.J.S.A. 2A:156A-1 to -37, because a telecommunications carrier may give police a user's location information upon presentation of a valid warrant. The Association contends that because of this facial compliance with the Act, geofence warrants may be constitutionally upheld and not improperly categorized as prohibited "general warrants" except where a reviewing court finds a specific proposed warrant too broadly drafted and rejects it on that basis.

In opposition, defendant argues the trial court correctly concluded the warrant was invalid and maintains Earls stands for the proposition "there is a reasonable expectation of privacy in [a cell phone user's] digital location

history," and, therefore, a geofence search requires a warrant supported by probable cause. He contends probable cause was lacking because the witnesses merely "speculated that the perpetrator may have been on the phone" without ever seeing one. Defendant further submits that since Earls was decided, a more pronounced right to privacy has emerged in federal case law, rendering geofence warrants invalid in all instances as unconstitutional general warrants that infringe upon the privacy rights of millions of people.

In the alternative, defendant offers a statistical argument to demonstrate the State did not establish probable cause sufficient to conduct the search, highlighting, at the time, Google's servers contained location data for "only one-third of Google users." As such, there was only a one-third chance that a given Google user has any location data on Google's server. And even if they did, a geofence search generates radius estimates with a confidence level of only 68%.

Further problematic, he claims, is the unsupported "string of inferences" necessary to arrive at the point at which those one-third and two-thirds figures apply. Specifically, (1) defendant had a Google account capable of recording his location to Google's server; (2) he opted-in to permit Google to record those estimates; (3) he had a functional phone on him at the time of the robbery; (4) his phone was a smartphone; (5) his smartphone had enabled GPS functionality;

and; (6) he was in fact logged into his Google account on that smartphone at the time of the robbery and generating location estimates.

Next, defendant argues the warrant lacked particularity, contending the State incorrectly frames this issue by focusing on whether the geographic area described by the warrant had "limited dimensions." Specifically, Google reports "any device that touches the geofence area," which artificially extends a geofence's parameters beyond what is listed in the warrant application. Defendant contends because a location estimate whose radius touched only the geofence's outer bounds would still be reported as responsive—even if the cell phone was mostly outside the radius—the State would still be permitted, under a warrant, to search tangential data that may not meet the probable cause standard. Defendant contends "Google could have been ordered to return data only for a device whose radius fell completely within the boundaries of the geofence. It was not ordered to do so." Failure to circumscribe the warrant in this way left open "the risk that people in cars traveling down the street without any connection to the robbery would be" reported as responsive to the warrant and therefore subject to criminal investigation.

Finally, defendant reiterates his argument before the trial court that before narrowing a given search, Google must search the location history of "hundreds

of millions of users and all of their devices, not just the devices in the gas station." It is uncontroverted Google began its analysis by reviewing information gathered from the accounts of 592 million users of Google's location history feature. Defendant argues the narrowness of the eventual seizure of one user's information does not transform the character of the search, which was overbroad and invalid at inception. In emphasizing this point, defendant highlights a recent case in which the Fifth Circuit held "geofence warrants are '[e]mblematic of general warrants' and are 'highly suspect per se.'" United States v. Smith, 110 F.4th 817, 838 (5th Cir. 2024) (alteration in original), reh'g en banc denied, No. 23-60321 (5th Cir. Jan. 14, 2025). Commenting on a procedure mirroring the three-step process present here, the Circuit Court stated:

> When law enforcement submits a geofence warrant to Google, Step 1 forces the company to search through its entire database to provide a new dataset that is derived from its entire Sensorvault. In other words, law enforcement cannot obtain its requested location data unless Google searches through the entirety of its Sensorvault—all 592 million individual accounts—for all of their locations at a given point in time. Moreover, this search is occurring while law enforcement officials have no idea who they are looking for, or whether the search will even turn up a result. Indeed, the quintessential problem with these warrants is that they never include a specific user to be identified, only a temporal and geographic location where any given user may turn up post-search. That is constitutionally insufficient.

> Geofence warrants present the exact sort of "general, exploratory rummaging" that the Fourth Amendment was designed to prevent.
>
> [Id. at 837 (footnote omitted).]

Defense amici, the American Civil Liberties Union ("ACLU"), ACLU of New Jersey, and Electronic Frontier Foundation, highlight the federal circuit split over whether geofence warrants implicate Fourth Amendment rights. Amici argue the State did not establish probable cause in this case because it "offered no evidence that the perpetrator of this crime would have data in" Google's server and, therefore, could not "justify the search of millions of users' location data" in an attempt to find the perpetrator's data. They write, "[g]eofence warrants suffer from . . . defects when they, like this one, are based on mere supposition that a suspect may have a phone, and that any given phone may share location data with Google." Finally, amici ask us to impose restraints limiting geofence warrants. Their argument includes itemized recommendations for our courts to follow when analyzing an application for a geofence warrant.

In this context, we note that whereas a warrant typically identifies a suspect and seeks evidence of a specific crime, geofence warrants seek evidence from a place where a crime has occurred. As the Fifth Circuit found in Smith, geofence warrants "never include a specific user to be identified, only a temporal

and geographic location where any given user may turn up post-search." 110 F. 4th at 837.

III.

The Fourth Amendment guarantees "the right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[3] U.S. Const. amend. IV. "The Fourth Amendment to the United States Constitution and Article I, Paragraph 7 of the New Jersey Constitution similarly protect citizens against unreasonable searches and seizures." State v. Gathers, 234 N.J. 208, 219 (2018). Reasonableness depends upon circumstances, balancing a search's "intrusion on the individual's Fourth Amendment interests against [the] promotion of legitimate governmental interests." Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 619 (1989) (quoting Delaware v. Prouse, 440 U.S. 648, 654 (1979)). The greater the intrusion, the "greater the level of protection" required by our state's constitution. Facebook, Inc. v. State, 254 N.J. 329, 364 (2023) (quoting State v. Lunsford, 226 N.J. 129, 131 (2016)). If "the State seeks to intrude upon an area in which our society

[3] The Fourth Amendment in full states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

recognizes a significantly heightened privacy interest, a more substantial justification is required to make the search 'reasonable.'" Winston v. Lee, 470 U.S. 753, 767 (1985).

A.

Status of Federal Law Regarding Geofence Warrants

We find no clear guidance in the federal law, where currently there exists a split amongst the federal circuits regarding the constitutionality of geofence warrants. A review of the relevant history of federal law demonstrates the United States Supreme Court has been grappling with applying Fourth Amendment protection over the last sixty years of technological advances. While the intent espoused in the Fourth Amendment has remained constant, its application has proven difficult in the face of technological advancements and has resulted in disparate rulings.

In Katz v. United States, 389 U.S. 347, 359 (1967), the Supreme Court ruled Katz was entitled to Fourth Amendment protection for the communications he made in a public phone booth. The Court clarified the Fourth Amendment protects people, not places, and the occurrence of a search is not dependent on physical intrusion. Id. at 353. Justice Harlan's concurrence set forth the seminal two-pronged "reasonable expectation of privacy" test courts continue to employ

today: (1) a person must have an actual, subjective expectation of privacy, and (2) the expectation is one "society is prepared to recognize as 'reasonable.'" Id. at 360-61 (Harlan, J., concurring).

In United States v. Miller, 425 U.S. 435, 443 (1976), the Court noted its previous decisions holding the Fourth Amendment does not prohibit law enforcement from obtaining information that has been revealed to a third party, even if that information was revealed under the assumption it would "be used only for a limited purpose" and the confidence placed in that third party would not be betrayed.

Subsequently, in Smith v. Maryland, 442 U.S. 735 (1979), the Court drew heavily from both Katz and Miller. See id. at 739-40, 743-45. Maryland involved a pen register,[4] installed pursuant to police request, that recorded the phone numbers dialed from Smith's home. Id. at 736-37. The pen register revealed a call had been placed from Smith's home to the victim's phone. Id. at 737. Police obtained a search warrant for his residence on that basis. The Court rejected Smith's effort to suppress the warrant, concluding that because the pen register did not acquire the contents of any communications, but rather the mere

[4] A pen register is a device that records the numbers dialed on a telephone through the monitoring of electrical impulses on a telephone. Pen registers do not relay oral communications or whether calls were completed. Id. at 736 n.1.

numbers dialed, Maryland was distinguishable from the type of listening device and resultant decision in Katz. Id. at 741. Applying the third-party doctrine, it further concluded there was no reasonable expectation of privacy in the dialed phone numbers because individuals do not possess a legitimate expectation of privacy in the numbers they dial as all phone users "realize that they must 'convey' phone numbers to the telephone company." Id. at 742.

In Steagald v. United States, 451 U.S. 204, 206-07 (1981), a Drug Enforcement Administration agent searched the home of Gaultney pursuant to an arrest warrant for Lyons. Steagald moved to suppress all evidence on the grounds it was illegally seized as the agents failed to obtain a search warrant prior to entering the home. Id. at 207. The Supreme Court reversed the judgments of the district court and Fifth Circuit denying the motion to suppress and remanded the case, emphasizing the Fourth Amendment prohibits the unfettered discretion posed by general warrants, concluding the officer's warrantless entry into a third-party's home, based on an arrest warrant for a person an informant alleged would be there, amounted to the very kind of unfettered discretion the Fourth Amendment is intended to guard against. Id. at 220-23.

In United States v. Knotts, 460 U.S. 276, 277-79 (1983), law enforcement relied on information obtained through both the use of a beeper[5] and visual surveillance to secure a search warrant for Knotts's cabin, which revealed contraband that resulted in his conviction. Knotts argued the use of the beeper to determine the chloroform can's presence on his property was a violation of his Fourth Amendment rights. Id. at 284. The Court held the monitoring of beeper signals, used to track the location of a chloroform canister was not a violation of the Fourth Amendment because visual surveillance would have revealed the same facts to the police. Id. at 282, 285. It held the Fourth Amendment does not prohibit police from augmenting their sensory faculties with the enhancement that technology affords them. Id. at 285.

In Kyllo v. United States, 533 U.S. 27, 29 (2001), federal agents used a thermal imager to scan the home of Kyllo, who was suspected of growing marijuana in his home. Relying on the resultant images showing some parts of the home to be relatively hot compared to others, the agents secured a search warrant authorizing a search of the home, where the agents found marijuana plants. Id. at 29-30. Kyllo was initially unsuccessful in his motion to suppress

[5] A beeper is a radio transmitter which emits signals. The beeper was placed in a chloroform can that was transported to the suspect's property by a co-defendant. Id. at 277-78.

the evidence obtained from his home. Id. at 30. The Supreme Court reversed and concluded "the information obtained by the thermal imager in this case was the product of a search." Id. at 34-35. The thermal imager was considered sense-enhancing technology that allowed officers to obtain information "regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area.'" Id. at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

In Carpenter v. United States, 585 U.S. 296, 301-02 (2018), police officers compelled Carpenter's wireless carriers to disclose his cell-site location information ("CSLI") and, relying on this information, charged Carpenter with six counts of robbery. Carpenter argued the Government's seizure of his CSLI violated the Fourth Amendment because the information had been obtained without a warrant. Id. at 302. The Government argued Carpenter lacked a reasonable expectation of privacy in the CSLI because he had voluntarily shared that information with his wireless carriers, and thus it was not subject to Fourth Amendment protection. See id. at 313. The Court rejected a mechanical application of the third-party doctrine but nevertheless found a search had occurred. Id. at 309-10, 314. The Court found the Government had failed to appreciate "there are no comparable limitations on the revealing nature of CSLI"

to cases which have previously been decided through the application of the third-party doctrine. Id. at 314.

In United States v. Smith, the Fifth Circuit concluded geofence warrants violate the Fourth Amendment because they are unconstitutional general warrants. 110 F.4th at 840. Smith involved the assault and robbery of a United States Postal Service ("U.S.P.S.") route driver while on his usual route. Id. at 820. The U.S.P.S. applied for a geofence warrant. The Step 3 request for de-anonymized information of three devices allowed the postal inspector to identify two suspects, who were charged. Id. at 828.

The defendants filed a motion to suppress evidence derived from the geofence warrant, which was denied. Id. at 829. After their conviction, the Fifth Circuit affirmed the district court's denial, even though it found geofence warrants unconstitutional, pursuant to the good-faith exception and "law enforcement's reasonable conduct . . . in light of the novelty of [geofence warrants]." Id. at 840.

In contrast, in United States v. Chatrie, the Fourth Circuit concluded the Government's use of a geofence warrant to obtain Chatrie's location information for the span of two hours did not constitute a search under the Fourth

Amendment because he had voluntarily provided this location information to Google when he signed onto location history. 107 F.4th at 321-22.

In Chatrie, after the initial investigation of a bank robbery was unsuccessful, law enforcement obtained a geofence warrant based upon security footage of the robbery which revealed the suspect was carrying a cell phone. Id. at 324. The requested warrant provided a geofence of a 150-meter radius surrounding the bank and included Google's three-step procedure for obtaining the location information. Id. at 324-25.

Pursuant to Step 1, law enforcement obtained 209 anonymized location data points from nineteen accounts within the designated geofence for an hour-long period. Id. at 324-25. For Step 2, Google provided law enforcement with 680 anonymized data points from nine accounts for a two-hour period. Id. at 325. Step 3 revealed identifying subscriber information for three accounts, one of which belonged to Chatrie, who was then indicted. Ibid.

Chatrie moved to suppress the evidence, which the district court denied but declined to address whether the evidence obtained violated the Fourth Amendment and instead relied upon the good-faith exception. Ibid. The Fourth Circuit noted law enforcement had obtained Chatrie's location information for a two-hour period, which was not "an 'all-encompassing record of [Chatrie's]

whereabouts . . . provid[ing] an intimate window into [his] person[al] life.'" Id. at 330 (alterations and omission in original) (quoting Carpenter, 585 U.S. at 311). Applying the third-party doctrine, the court concluded Chatrie "did not have a 'legitimate expectation of privacy,' in the" location information obtained by law enforcement. Id. at 331 (quoting Carpenter, 585 U.S. at 314) (internal quotation marks omitted). Further, the court concluded Chatrie voluntarily provided his location information to Google when he chose to opt in to location history. Ibid. The court distinguished CSLI from location history because a user must consent to this setting and thus "knowingly and voluntarily expose[] his [l]ocation [h]istory data to Google." Ibid. Additionally, the court ruled location history is not as pervasive or indispensable to modern society as a cell phone because location history is not needed to use a cell phone or to use Google applications. Id. at 331-32. The Fourth Circuit concluded location history is obtained only after a user's consent to the technology, and Chatrie "knowingly and voluntarily chose to allow" the collection and storage of his location information, thus law enforcement did not conduct a search. Id. at 332.

Following an en banc rehearing, seven of fifteen judges concurred in this assessment. Writing in concurrence, Judge Wilkinson observed:

> With due regard for my fine colleagues, there was no search here. And even if one were to assume there was

> a search, there are many good reasons why courts should respectfully reject the assault on geofence warrants mounted by appellant, several of my colleagues; see opinion of Wynn, J. (concurring), and the Fifth Circuit Court of Appeals; see Smith, 110 F.4th 817.
>
> [Chatrie, ___ F.4th at ___ (slip op. at 21) (Wilkinson, J., concurring) (citation reformatted).]

Finally, in Rhine, the district court denied Rhine's motion to suppress evidence obtained through a geofence warrant. 652 F. Supp. 3d at 45-46. Rhine involved the defendant's participation in the January 6, 2021 riot at the Capitol building. Ibid. The Government alleged Rhine was a part of the crowd who were gathered outside of the Capitol and was among those who started to force their way into the building. Id. at 46. After requesting a geofence warrant for the location information of cell phones that were in or immediately around the Capitol on January 6, 2021, from 2:00 p.m. to 6:30 p.m., the Government obtained Rhine's Google location history data. Id. at 66. Rhine argued that the geofence warrant law enforcement obtained was overbroad and lacking in particularity. Ibid.

The district court found the geofence warrant was "supported by particularized probable cause" and "its alleged infirmities would fall into the good faith exception to the exclusionary rule." Id. at 81. It declined to decide

whether there was a Fourth Amendment search because it denied Rhine's motion to suppress on other grounds. Ibid. Nevertheless, the court disagreed with Rhine's contention that Step 1 of Google's three-step procedure was overly broad as it required Google to search millions of accounts without probable cause because the "relevant question is not how Google runs searches on its data, but what the warrant authorizes the Government to search and seize." Id. at 82.

The district court found Rhine's argument regarding Step 2 unpersuasive as well because the lists Google provided to law enforcement consisted of anonymized data which was authorized by the warrant. Id. at 84. Addressing Step 3, the court ruled "[b]ased on an unusual abundance of surveillance footage, news footage, and photographs and videos taken by the suspects themselves while inside the Capitol building, there is much more than a 'fair probability' that the suspects were within the geofence area and were carrying and using smartphones while there," providing probable cause that their cell phones' location history would offer evidence of a crime. Id. at 84-85. Further, the court found law enforcement's efforts to narrow the "step three universe" were reasonable and effective. Id. at 85-86. The court noted the four-and-a-half-hour time period itself was not unreasonable because it was corroborated by timelines of the January 6 riot at the Capitol. Id. at 88.

This review of federal law underscores the lack of any consensus we may use as guidance. At the same time, it contains approaches on which we base our holding.

B.

New Jersey Law

Although our review of the denial of a suppression motion is generally "circumscribed," we do not uphold a trial court's granting of a motion to suppress when its findings are not "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) (internal quotation marks omitted)). Accordingly, any deference to the trial court is forsaken when the trial court's findings are "'so clearly mistaken "that the interests of justice demand intervention and correction." Ibid. (quoting State v. Elders, 192 N.J. 224, 244 (2007) (internal quotation marks omitted)). 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).

It is well established that a trial court, considering a motion to suppress evidence obtained based upon a search warrant, owes substantial deference to

the warrant. See State v. Kasabucki, 52 N.J. 110, 117 (1968). A search warrant enjoys a presumption of validity. State v. Bivins, 226 N.J. 1, 11 (2016); State v. Marshall, 199 N.J. 602, 612 (2009). "[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. Evers, 175 N.J. 355, 381 (2003). 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). "[W]hen the adequacy of the facts offered to show probable cause . . . appears to be marginal, the doubt should ordinarily be resolved by sustaining the search." Kasabucki, 52 N.J. at 116.

Like the United States Constitution, the New Jersey Constitution protects an individual from unreasonable searches and seizures. U.S. Const. amend. IV; N.J. Const. art. I, ¶ 7.[6] Generally, the inquiry regarding whether a search warrant is necessary depends on whether the individual has a reasonable expectation of privacy in the information obtained. See State v. McQueen, 248 N.J. 26, 42

[6] Article 1, Paragraph 7 of the New Jersey Constitution reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrant shall issue except upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the papers and things to be seized."

(2021). "[E]xpectations of privacy are established by general social norms." State v. Hempele, 120 N.J. 182, 200 (1990); see also State v. Williams, 461 N.J. Super. 1, 12 (App. Div. 2019), aff'd, 244 N.J. 327 (2020).

In State v. Reid, the State alleged the defendant logged onto the website of her employer's business supplier from her home computer and changed her employer's password and shipping address to a nonexistent location in an act of retaliation. 194 N.J. 386, 389 (2008). The supplier's website captured the defendant's IP address and gave that information to her employer, who turned it over to police. Ibid. A municipal court issued a subpoena to Comcast seeking information relating to the IP address during the three-hour period the supplier's website was accessed. Id. at 392-93. In response to the subpoena, Comcast identified the defendant as the subscriber for the IP address and provided the defendant's address and telephone number. Id. at 393. The defendant was arrested and charged with second-degree computer theft. N.J.S.A. 2C:20-25(b). Ibid.

The defendant moved to suppress the information obtained through the subpoena. Both the trial court and this court suppressed the information, finding, among other things, the defendant had an expectation of privacy in her internet subscriber information. Id. at 393-94. Our Supreme Court affirmed.

Id. at 407. The Court noted that in the preceding "twenty-five years, a series of New Jersey cases has expanded the privacy rights enjoyed by citizens of this state." Id. at 397. The Court stated in one case, State v. Hunt, 91 N.J. 338 (1982), it found "telephone toll billing records are 'part of the privacy package'" protected from a warrantless search. Reid, 194 N.J. at 397 (quoting Hunt, 91 N.J. at 347). In Hunt, the Court observed "[t]he telephone has become an essential instrument in carrying on our personal affairs," and that a list of telephone numbers dialed in the privacy of one's home "could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life." 91 N.J. at 346-47 (quoting Maryland, 442 U.S. at 748 (Stewart, J., dissenting)). See Reid, 194 N.J. at 397. In addition, the Court noted a person "is entitled to assume that the numbers he dials in the privacy of his home will be recorded solely for the telephone company's business purposes." Hunt, 91 N.J. at 347.

The Reid Court noted:

> With a complete listing of IP addresses, one can track a person's Internet usage. "The government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's . . . fantasies, her health concerns, and so on." Daniel Solove, The Future of Internet Surveillance Law, 72 Geo. Wash. L. Rev. 1264, 1287 (2004). Such information can reveal intimate details about one's

> personal affairs in the same way disclosure of telephone billing records does. Although the contents of Internet communications may be even more revealing, both types of information implicate privacy interests.
>
> [Reid, 194 N.J. at 398-99 (omission in original) (citation reformatted).]

The Court specifically rejected the application of the third-party doctrine employed by federal courts. Id. at 399. "Under our precedents, users are entitled to expect confidentiality under these circumstances." Ibid.

In State v. Earls, our Supreme Court considered "whether people have a constitutional right of privacy in cell-phone location information." 214 N.J. at 568. In Earls, an officer obtained an arrest warrant for the defendant, who police believed was with his endangered girlfriend. Id. at 571. In an effort to find them, the officer contacted T-Mobile, the service provider for a cell phone believed to be in the defendant's possession. Ibid. Three times that evening, T-Mobile provided information about the location of the cell phone via cell phone tower transmissions without a search warrant. Ibid. Ultimately, the officer located the defendant and his girlfriend at a motel, where a search of their luggage revealed stolen property and marijuana. Id. at 572. The defendant was arrested and charged with several offenses. Ibid.

The defendant moved to suppress the information provided by T-Mobile, arguing he had a reasonable expectation of privacy in his cell phone location data, requiring the officer to obtain a search warrant before securing his location data from his service provider. Id. at 573-74. The trial court and this court denied the defendant's motion to suppress. Ibid.

The Supreme Court reversed. Id. at 593. It found:

> 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 noted cell phones "blur the historical distinction between public and private areas" and CSLI "does more than simply augment visual surveillance in public areas." Ibid. Finally, the Court observed,

> cell-phone use has become an indispensable part of modern life. The hundreds of millions of wireless devices in use each day can often be found near their owners—at work, school, or home, and at events and gatherings of all types. And wherever those mobile devices may be, they continuously identify their location to nearby cell towers so long as they are not turned off.
>
> [Id. at 586-87.]

The Court also found

> 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.]

The Court concluded:

> For the reasons discussed, we conclude Article I, Paragraph 7 of the New Jersey Constitution protects an individual's privacy interest in the location of his or her cell phone. Users are reasonably entitled to expect confidentiality in the ever-increasing level of detail that cell phones can reveal about their lives. Because of the nature of the intrusion, and the corresponding, legitimate privacy interest at stake, we hold today that 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.]

It is important to note Earls involved a warrantless search. See id. at 592. Despite the heightened privacy interest in cell phone location addressed in Earls, the Supreme Court did not foreclose the possibility of law enforcement obtaining this information. Id. at 589. Indeed, the Court specifically recognized law enforcement's ability to obtain cell phone location information through the use of an appropriate warrant, notwithstanding an individual's reasonable expectation of privacy. Ibid.

As described by the United States Supreme Court in Mincey v. Arizona, 437 U.S. 385 (1978), another case involving a warrantless search, the Court noted an appropriate warrant would have allowed the search.

> It may well be that the circumstances described by the Arizona Supreme Court would usually be constitutionally sufficient to warrant a search of substantial scope. But the Fourth Amendment requires that this judgment in each case be made in the first instance by a neutral magistrate.
>
> "The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."
>
> [Id. at 395 (quoting Johnson v. United States, 333 U.S. 10, 13-14 (1948)).]

IV.

A.

Probable Cause for Warrant I

The hallmarks of a valid warrant are "probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness." Zurcher v. Stanford Daily, 436 U.S. 547, 565 (1978). "To conduct a search, the State ordinarily must demonstrate there is probable cause to believe evidence of a crime will be found at a particular place and must obtain a warrant." Facebook, Inc., 254 N.J. at 340. The probable cause standard balances law enforcement's interest in "fair leeway for enforcing the law" against the public's interest in freedom "from rash and unreasonable interferences with privacy and from unfounded charges of crime." Brinegar v. United States, 338 U.S. 160, 176 (1949).

Probable cause "eludes precise definition." Gathers, 234 N.J. at 220 (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." State v. Missak, 476 N.J. Super. 302, 321 (App. Div. 2023) (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.

Courts must take "a practical and realistic" approach to evaluating the probable cause showing in a search warrant application. Kasabucki, 52 N.J. at 117. Generally, the court confines its analysis to "the four corners of the supporting affidavit, as supplemented by sworn testimony before the issuing judge." Missak, 476 N.J. Super. at 316-17 (quoting Marshall, 199 N.J. at 611). Yet, the analysis also considers "all relevant circumstances," Gathers, 234 N.J. at 221 (quoting Keyes, 184 N.J. at 554), and "reasonable and natural inferences" flowing therefrom. Evers, 175 N.J. at 384. The "facts asserted must be tested by the practical considerations of everyday life on which reasonably prudent and experienced police officers act." Kasabucki, 52 N.J. at 117.

Binding caselaw recognizes cell phones are "now 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 "significant majority of American adults now own such

phones." Ibid.; see also Earls, 214 N.J. at 579 ("[In] May 2013, the Pew Research Center reported that 91 percent of American adults have a cell phone and 56 percent have a smartphone.").

Given the recognized widespread use of cell phones and the unavailability of public phones, the State is correct that it need not prove defendant was using a cell phone in order to establish probable cause to obtain a geofence warrant. Indeed, in search warrants where the identity of the suspect is known, law enforcement need not prove the suspect owns or was using a cell phone at the time of the commission of the crime in order to obtain potentially relevant evidence from that suspect's cell phone. Law enforcement regularly relies upon the presumption that most people have cell phones and support their warrant applications with other evidence establishing probable cause. As noted in Earls, twelve years ago, 91 percent of Americans had cell phones and over half had smart phones. 214 N.J. at 579.

Nonetheless, we agree with the State that the record allows a reasonable "inference the defendant was engaged in a telephone conversation based upon the account of both" the victim and the customer, who stated they "overheard a detailed conversation regarding a woman smoking marijuana while pregnant." In its ruling, the trial court stated the affidavit was premised on preconceptions

originating from the standards and customs of one's own culture and lifestyle. Simply stated, "just because you and others around you have cellular telephone[s] doesn't mean that everyone has one. People live in a variety of lifestyles defined by the economic, social, and cultural influences specific to them. As a result, [the detective's] assertion[s] fall[] short of what is required for probable cause."

In making that finding, the motion court was mistaken in not adequately accounting for the practical realities of everyday life. The court erroneously based its legal conclusion on the notion it was presumptuous for the court issuing the search warrant in this case to infer defendant possessed a cell phone. The trial court's conclusion that the search warrant lacked probable cause because no one had actually seen the cell phone ignored the pervasive use of ear buds and cellular watches in today's society. The record supports the existence of probable cause based on the conclusion the perpetrator was using a cell phone, as certified by two witnesses. See Keyes, 184 N.J. at 560 ("'[T]he fact that the police were unable to observe the informant enter [the apartment] itself does not prevent a finding of probable cause' . . . . [It] is just another factor the court should consider under the totality of the circumstances analysis." (quoting State v. Sullivan, 169 N.J. 204, 216 (2001))). On the basis of two witnesses'

statements, two different Superior Court judges found there to be probable cause to believe a search of cell phone location presence would lead to evidence identifying the perpetrator or witnesses of the crime.

Moreover, Warrant I was narrowly tailored as to time and place and likely to lead to the discovery of evidence. It sought information for the limited duration of fourteen minutes, a time corroborated by the store's surveillance footage. It did not seek location tracking but rather location presence of any cellular devices within the convenience store during that brief window of time. And whether Warrant I identified anonymous information for one cell phone or four, police were able to ascribe the other phones to the employees and witnesses present in the store during that timeframe.

Our esteemed colleague dissents, concluding there was insufficient probable cause to believe the device would have been logged onto location history at the time of the robbery and assault. Accordingly, Warrant I was based on a "hunch." We respectfully disagree. The record demonstrates approximately thirty-three percent of Google users affirmatively authorize location history.[7] We decline to adopt our dissenting colleague's view that is

[7] Our dissenting colleague is correct in observing this fact is beyond the four corners of the affidavit in support of Warrant I. Instead, we reference this figure

tantamount to holding that for probable cause to exist, police must first link a cell phone to the type of specific cellular technology in use—location history in this instance. With such a requirement, no CDW warrant would ever issue, in any matter, because law enforcement will never know the precise applications, programs, or information contained on a particular cell phone at the time it applies for a search warrant.

Consider a like scenario where there is no doubt the suspected perpetrator was using a smart phone as shown on a surveillance video. How would police go about obtaining geofence information from a service provider with a warrant? To which service provider should the warrant be directed? Investigative work necessarily entails a string of reasonable inferences that do not require a given percentage of assured success, only a reasonable likelihood of leading to evidence identifying the perpetrator or witnesses of a crime. Is this highly relevant information categorically constitutionally inaccessible because police do not have probable cause in advance to believe location history was activated on the perpetrator's phone?

---

as presented to the motion court for context as to what constitutes a reasonable inference that may be made as drawn from common sense and experience.

Presented otherwise, if the prosecutor receives an approved CDW for Google, and Google determines it has no information regarding the time and location requested, what privacy right has been violated? What private information has been disclosed? Utilizing Google's vetted three-step process, Google is first asked if it has any information regarding a cell phone's presence at that time and location, and, if the answer affirmative, it is then asked to narrow down the number of users at the time and location, and, after further investigation, to disclose the identity of the user(s). The privacy interests of the citizenry are not implicated until this third stage, well after initial probable cause is established, and only after two more stages of probable cause are judicially sanctioned.

Privacy, Particularization, and Probable Cause

As with technology, concepts of privacy interests and particularization evolve. In his recent Chatrie concurrence, Judge Wilkinson articulated an expanded conception of privacy:

> So yes, the Bill of Rights stands vigilant guard against the abuses of the state. The Fourth Amendment is itself a prime illustration of its function. Yet privacy is also threatened by, say, a theft of personal items. And privacy is in part a peace of mind. The prospect of criminal malefactors intruding on that peace can only mean our privacy has been compromised. That the transgression is attributable to private actors does not

> mean it cannot be part of the calculus of reasonableness which, again, is our Fourth Amendment touchstone. Seen in this light, privacy is not invariably in an adversarial relationship with the state, but something the state can take measured steps to protect and provide.
>
> [Chatrie, ___ F.4th at ___ (slip op. at 23-24) (Wilkinson, J., concurring).]

Particularly pertinent to this circumstance, our highest Court addressed the question of probable cause arising from the presence of a suspect in a particular place at a given time. Because Chief Justice Weintraub ably explained how probable cause so grounded does not amount to a general warrant, we quote his analysis at length:

> The majority of the Appellate Division cited State v. Masco, 103 N.J. Super. 277 (App. Div. 1968). There the search warrant issued on a showing of probable cause that horse race bets were being taken by an unknown man in a one-family dwelling. The warrant directed a search, for gambling paraphernalia, of the dwelling "and the person of those found within" it. The search of the individual found on the premises was sustained as incidental to a valid arrest based upon probable cause the officer found at the scene, but the warrant was thought to be invalid insofar as it authorized a search of persons found on the premises. The basis of that view was not a lack of probable cause but rather that the warrant was a "general" warrant because it did not describe the persons to be searched with the specificity required by the Fourth Amendment.
>
> On principle, the sufficiency of a warrant to search persons identified only by their presence at a specified

place should depend upon the facts. A showing that lottery slips are sold in a department store or an industrial plant obviously would not justify a warrant to search every person on the premises, for there would be no probable cause to believe that everyone there was participating in the illegal operation. On the other hand, a showing that a dice game is operated in a manhole or in a barn should suffice, for the reason that the place is so limited and the illegal operation so overt that it is likely that everyone present is a party to the offense. Such a setting furnishes not only probable cause but also a designation of the persons to be searched which functionally is as precise as a dimensional portrait of them.

As to probable cause, it must be remembered that the showing need not equal a prima facie case required to sustain a conviction. No more is demanded than a well-grounded suspicion or belief that an offense is taking place and the individual is party to it. State v. Burnett, 42 N.J. 377, 386-388 (1964); State v. Davis, 50 N.J. 16, 23-24 (1967). And, with regard to the Fourth Amendment demand for specificity as to the subject to be searched, there is none of the vice of a general warrant if the individual is thus identified by physical nexus to the on-going criminal event itself. In such a setting, the officer executing the warrant has neither the authority nor the opportunity to search everywhere for anyone violating a law. So long as there is good reason to suspect or believe that anyone present at the anticipated scene will probably be a participant, presence becomes the descriptive fact satisfying the aim of the Fourth Amendment. The evil of the general warrant is thereby negated. To insist nonetheless that the individual be otherwise described when circumstances will not permit it, would simply deny government a needed power to deal with crime, without

> advancing the interest the Amendment was meant to serve.
>
> [State v. De Simone, 60 N.J. 319, 321-22 (1972) (emphases added and italicization omitted) (citations reformatted).]

Here, concern for the general public's right to privacy is safeguarded through the three-step process. In the end, only the suspect(s) or witness(es) are identified through a technology that provides "a designation of the persons to be searched which functionally is as precise as a dimensional portrait of them." Id. at 322. The vice of a general warrant is eliminated through the precise geographic and temporal parameters and the winnowing steps of geofence warrants.

Continuing in this vein, Chief Justice Rabner foresaw these advances in technology in State v. Reid. The Chief Justice presciently commented that what society views as reasonable, under the reasonable expectation of privacy test, can change as new technologies become available. That change may not always be an expansion of privacy rights and might instead lead to a lessening of the restrictions placed on law enforcement.

Writing for a unanimous Court, the Chief Justice forecasted:

> One additional point bears mention about the right to privacy in ISP subscriber information: the reasonableness of the privacy interest may change as

> technology evolves. A reasonable expectation of privacy is required to establish a protected privacy interest. Hempele, 120 N.J. at 220. As discussed . . . , Internet users today enjoy relatively complete IP address anonymity when surfing the Web. Given the current state of technology, the dynamic, temporarily assigned, numerical IP address cannot be matched to an individual user without the help of an ISP. Therefore, we accept as reasonable the expectation that one's identity will not be discovered through a string of numbers left behind on a website.
>
> The availability of IP Address Locator Websites has not altered that expectation because they reveal the name and address of service providers but not individual users. Should that reality change over time, the reasonableness of the expectation of privacy in Internet subscriber information might change as well. For example, if one day new software allowed individuals to type IP addresses into a "reverse directory" and identify the name of a user—as is possible with reverse telephone directories—today's ruling might need to be reexamined.
>
> [Reid, 194 N.J. at 401-02 (emphases added and italicization omitted) (citation reformatted).]

For probable cause in support of a warrant to be found, proof beyond a reasonable doubt is not required; nor is a preponderance of the evidence necessary. To be sure, a search warrant cannot be issued on a "hunch," but all that is required for "[p]robable cause for the issuance of a search warrant [is] 'a fair probability that contraband or evidence of a crime will be found in a particular place.'" State v. Chippero, 201 N.J. 14, 28 (2009); see also Evers, 175

N.J. at 381 (requiring the issuing judge to find "that a crime has been or is being committed at a specific location or that evidence of a crime is at the place to be searched"); State v. Moore, 181 N.J. 40, 45 (2004) (describing the standard as requiring a well-grounded suspicion). The judge's inquiry with respect to a search warrant is to "assess the connection of the item sought to be seized 1) to the crime being investigated, and 2) to the location to be searched as its likely present location." Chippero, 201 N.J. at 29.

Our conclusion that Warrant I was based on sufficient probable cause, requiring the trial court to examine the sufficiency of Warrants II and III, is consistent with the Supreme Court's holding in Earls, albeit where the identity of the defendant was already known:

> We also recognize that cell-phone location information can be a powerful tool to fight crime. That data will still be available to law enforcement officers upon a showing of probable cause. To be clear, the police will be able to access cell-phone location data with a properly authorized search warrant.
>
> [214 N.J. at 569.]

Merely because one maintains a reasonable expectation of privacy does not conclusively enjoin law enforcement's ability to search as "the permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate

governmental interests." State v. Terry, 232 N.J. 218, 222-23, 232 (2018) (quoting Prouse, 440 U.S. at 654) (concluding the trial court did not err in denying defendant's motion to suppress a handgun found in his glove compartment when law enforcement searched for proof of ownership despite his privacy interest in the car); see also Keyes, 184 N.J. at 557-60 (holding a warrant to search defendant's residence for drugs based on an informant's tip properly had probable cause, despite officers' inability to see the informant enter defendant's residence, by "accomodat[ing] th[e] often competing interests of [an individual's privacy interest and law enforcement's legitimate crimefighting interests] so as to serve them both in a practical fashion without unduly hampering the one or unreasonably impairing the significant content of the other" (quoting Kasabucki, 52 N.J. at 116)). Here, the intrusion upon defendant's privacy was minimal, as Warrant I sought any cell phone's presence, not location tracking, at a public location where individuals were already subject to video surveillance. That intrusion must be balanced against law enforcement's obligation to investigate crime, a legitimate governmental interest.

Furthermore, we reject the argument that Warrant I was a general warrant because it purportedly violated the right to privacy of millions of cell phone

users. Defendant and defense amici continually reference the 592 million subscribers who must be necessarily "searched" in order to respond to the warrant. We disagree. First, pursuant to the three-step process Google had instituted after vetting with the DOJ, which is similar to the process New Jersey authorized for search warrants of license plate reader information, see Off. of the Att'y Gen., Law Enf't Directive No. 2022-12, Updated Directive Regulating Use of Automated License Plate Recognition (ALPR) Technology (Oct. 21, 2022), Google ascribes a non-identifying unique identifier for all users who opt into location history. Thus, no individual's identifying information is known, even to Google, pursuant to Step 1 or 2. Google obtains identifying information only at Step 3. Moreover, Google conducts that search of its own proprietary data. That data belongs to Google, which may search its proprietary information in any way consistent with its user agreements. It may share the results of the search or even sell it, as long as its search and subsequent use of the data is consistent with its contractual agreements with its users.

We conclude geofence warrants are not unconstitutional per se and instead, pursuant to Earls, require a case-by-case examination of the facts supporting the probable cause for the issuance of each warrant involved in the three-step process. With respect to Warrant I, we conclude the trial court's

finding of probable cause should have been upheld by the trial court reviewing the motion to suppress, which owed greater deference to the validity of the warrant. See Bivins, 226 N.J. at 11.

B.

Probable Cause Regarding Warrants II and III

Although we believe the general means employed with respect to this particular case served to minimize—even eliminate—perceptible intrusion on the privacy interests of the public in an effort to solve a violent and otherwise unsolvable crime, the trial court reviewing the motion to suppress did not perform any analysis of the probable cause involved in the issuance of Warrants II and III.

We acknowledge the expectation of privacy in a cell phone users' location history and movements, and our Supreme Court specifically rejected the third-party doctrine in Reid, 194 N.J. at 399. Our Court also specifically rejected the good-faith exception, granting individuals in New Jersey more protection than the U.S. Constitution. Compare United States v. Leon, 468 U.S. 897 (1984), with State v. Boone, 232 N.J. 417 (2017).

However, the trial court did not analyze whether defendant's reasonable expectation of privacy in his presence at the gas station, a place where his image

was captured on video, was overcome by law enforcement's competing interest or whether the geofence radius was sufficiently narrowly-tailored to exclude location history for anyone who might have been identified but was not in the store at the time of the robbery and assault.

By way of illustration only, if there existed a private apartment above the gas station, the trial court issuing the second warrant would have had to analyze whether the results of the geofence search potentially identified a person in that apartment above the store, and not merely persons in the gas station. Certainly, if the second warrant tracked defendant's movements outside the store in a direction inconsistent with the gas pump attendant's testimony regarding the direction in which the suspect fled, the second warrant may have lacked probable cause. Finally, if the results of the first warrant had returned a number of cell phones not consistent with the number of people in the store at the time of the robbery, as corroborated by surveillance video footage, the second and third warrants may have been impermissibly over-broad. A fact-based analysis of each warrant in Google's three-step procedure is critical to search warrants issued pursuant to geofence technology.

The trial court also did not address whether Warrant II specifically identified defendant's cell phone as within the confines of the convenience store

and not adjacent to it during the applicable time period. Nor did the court consider why other cell phones within the geofence were not identified in Google's search, including those belonging to the victim, the customer, and the gas pump attendant standing outside the store and presumably within the geofence perimeter. This inquiry would address the reliability of the data and whether the warrants were reasonably tailored to lead to the discovery of admissible evidence. It would also address the concerns raised by defendant regarding the potential identification of an individual who may be driving by and inadvertently caught within the geofence.

We have no information as to the probable cause for the issuance of Warrant III, which provided extensive cell phone data to law enforcement. For these reasons, we are constrained to remand for a new suppression hearing.

C.

Situs of the Crime Scene Warrant

Finally, we question whether geofence warrants should be treated as search warrants of a place to be searched. Like a search warrant of the location of a crime for blood, hair fibers, or other DNA evidence, a geofence warrant searches the location of a crime for the presence of any cellular device at the crime scene at a particular point in time.

In this manner, cellular database searches most resemble routine criminal investigations in which police search phone numbers, license plates numbers, or DNA profiles. When investigators conduct investigations of this type, they run determined search criteria and then review the results. They do not examine every license plate, phone number, or DNA sequence. Thus, privacy of information not pertinent to the search query is not exposed for examination by the investigator because it is excluded from capture and consequent exposure by the search criteria employed. It is inaccurate to maintain that information in a database that was not returned by way of search result was "searched" at all. See Camara v. Mun. Ct. of City & Cnty. of S.F., 387 U.S. 523, 528 (1967) ("The basic purpose of th[e Fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.").

As the Georgia Supreme Court recently observed:

> The possibility that the access the warrant authorized could also allow the police to view anonymized data not associated with the suspect does not affect the probable-cause assessment, which turns on the likelihood that the access granted by the warrant could lead to the suspect's identity. Nor does that possibility on its own make this warrant overbroad—just as a search warrant for a person's papers is not overbroad because not all of the documents examined will be evidence of a crime. See Andresen v. Maryland, 427

> U.S. 463, 482 n.11 (1976) (recognizing that when a search warrant authorizes the search and seizure of a person's papers, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized"); United States v. Ulbricht, 858 F.3d 71, 100 (2d Cir. 2017) ("[T]raditional searches for paper records, like searches for electronic records, have always entailed the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are."), abrogated on other grounds by Carpenter, 585 U.S. at 309-310.
>
> [Jones v. State, ___ S.E.2d ___, ___ (Ga. 2025) (slip op. at 24-25) (emphasis added) (citations reformatted).]

V.

In sum, the order granting defendant's motion to suppress evidence is vacated and the matter is remanded for a new suppression hearing to perform a probable cause analysis with respect to Warrants II and III. Because the August 8, 2024 release order was premised on the suppression order, we vacate that release order and our stay of that order, with no prejudice to defendant renewing his motion in the future.

Vacated and remanded. We do not retain jurisdiction.

GUMMER, J.A.D., dissenting.

Was the finding of probable cause for the issuance of the first warrant (Warrant I) supported by adequate facts? That is the narrow, threshold question before this court. Because I am convinced the suppression-motion judge correctly answered that question in the negative, I respectfully dissent.

A court's "probable cause determination must be . . . based on the information contained within the four corners of the supporting affidavit . . . ." State v. Missak, 476 N.J. Super. 302, 316-17 (App. Div. 2023) (first omission in the original) (quoting State v. Marshall, 199 N.J. 602, 611 (2009))[1]; see also State v. Sims, 75 N.J. 337, 350 (1978) (holding "[c]rucial to that [probable-cause] determination are the specific facts placed before the judge at the time the warrant is sought"). A court also must "consider the totality of the circumstances and should sustain the validity of a search only if the finding of probable cause relies on adequate facts." Missak, 476 N.J. Super. at 317 (quoting State v. Boone, 232 N.J. 417, 427 (2017)) (internal quotation marks omitted). "The suppression motion judge's findings should be overturned 'only if they are so clearly mistaken that the interests of justice demand intervention

---

[1] A court may also consider "sworn testimony [given] before the issuing judge that [wa]s recorded contemporaneously." Ibid. (quoting Marshall, 199 N.J. at 611). No such testimony was given in this case.

and correction.'" Boone, 232 N.J. at 426 (quoting State v. Elders, 192 N.J. 224, 244 (2007)) (internal quotation marks omitted).

Thus, our determination of the question before the court should begin, and potentially end, with a review of the information the detective provided in the certification he submitted in support of his application for Warrant I. In that certification, the detective explained the process he anticipated law-enforcement officers would follow after receiving Google's response to the warrant. He provided information regarding his professional experience. He also set forth what he described as "FACTS IN SUPPORT OF PROBABLE CAUSE." Some of those facts related to the alleged armed robbery at the gas service station; some related to cell phones and Google.

Regarding the robbery, the detective certified a female employee who worked behind the register of a store located within the gas service station complex had advised police officers who arrived on the scene "the store had just been robbed." She described the suspect to the officers and told them she believed he "was speaking to someone on a cell phone using ear buds." According to the employee, "it seemed like [he] was speaking to a female who was pregnant because he was stating something to the effect that it was not a good idea for her to smoke while she was pregnant." On March 17, 2022, the

detective spoke with a customer who was in the store before the robbery occurred. She told the detective the suspect had allowed her to go in front of him to make a purchase and that while she was standing there, she had heard him "talking to someone as if he was on the phone because he was not talking to her or the employee."

In the "FACTS IN SUPPORT OF PROBABLE CAUSE" section of his certification, the detective provided the following information regarding cell phones:

> 19. Your Affiant knows that most people in today's society possess a cellular telephone or mobile telephone, which is a handheld, wireless device primarily used for voice, text, and data communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called "cells" or "cell sites," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") or other technology for determining a more precise location of the device. I know that most people will carry them whenever they leave their place of residence.

He provided the following information regarding Google:

> 20. This applicant also knows that Google, Inc. is a company which, among other things, provides

electronic communication services to subscribers, including email services. Google allows subscribers to obtain email accounts at the domain name gmail.com and/or google.com. Subscribers obtain an account by registering with Google. A subscriber using the Provider's services can access his or her email account from any computer/device connected to the Internet.

21. This applicant knows that Google has also developed a proprietary operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

22. Based on this applicant's training and experience, this applicant knows that Google, Inc. collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled. The company uses this information for location-based advertising and location-based search results and stored such data in perpetuity unless it is manually deleted by the user. This location information is derived from GPS data, cell site/cell tower information, Bluetooth connections, and Wi-Fi access points.

23. This applicant knows that location data can 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. Such information can also aid investigators in possibly inculpating or exculpating persons of interest.
>
> 24. Additionally, location information can be digitally integrated into image, video, or other computer files associated with a Google account and can indicate the geographic location of the account[']s user at a particular date and time (e.g., digital cameras, including on cellular telephones, frequently store GPS coordinates indicating where a photo was taken in the "metadata" of an image file).

Based on those facts,[2] Warrant I was issued.

For the motion judge, the information contained in the certification the detective submitted in support of the issuance of Warrant I – what the judge characterized as the detective's unsupported assertions about most people possessing cell phones and most people carrying them with them and the

---

[2] In holding probable cause supported the issuance of Warrant I, the majority considers information not included in the detective's certification. For example, the majority considers that "[t]he record demonstrates approximately thirty-three percent of Google users affirmatively authorize location history." Ante at ___ (slip op. at 48). But that factual assertion, as the majority concedes, id. at 48 n.7, was not "within the four corners of the supporting affidavit," Missak, 476 N.J. Super. at 316-17 (quoting Marshall, 199 N.J. at 611), and it was not one of "the specific facts placed before the judge at the time the warrant [wa]s sought," Sims, 75 N.J. at 350. And, contrary to the majority's assertion, it is not "reasonable" to infer "from common sense and experience" the very specific statistic that "thirty-three percent of Google users affirmatively authorize location history." Ante at ___ (slip op. at 48 & n.7).

witnesses' "supposition" the suspect had a cell phone and ear buds even though they had not seen either – was not enough to support the factual conclusion the suspect possessed a cell phone. On that record, I cannot say the motion judge's determination was "so clearly mistaken that the interests of justice demand intervention and correction." Boone, 232 N.J. at 426 (quoting Elders, 192 N.J. at 244) (internal quotation marks omitted).

But even if I were to accept the conclusion the suspect had the unseen cell phone and ear buds with him at the time of the robbery, I see nothing in the detective's certification or the surrounding circumstances that supports the next step: issuing a warrant to Google. Contrary to the majority's holding, the conclusion the suspect possessed a cell phone does not support a finding of probable cause for the issuance of a warrant to Google. See ante at ___ (slip op. at 47) ("The record supports the existence of probable cause based on the conclusion the perpetrator was using a cell phone, as certified by two witnesses."). The detective's certification provides no nexus between the suspect having a phone and Google having information about the suspect. The detective described Google's operating system and its collection of location data but does not link Google to this suspect or this crime or this gas service station.

The bridge between the suspect and Google is built on a series of assumptions: defendant had a Google account capable of recording his location to Google's server; he had opted-in to permit Google to record the estimates of his location; the user agreement between Google and defendant, which is not in the record, provides the location "data belongs to Google" and authorized Google to "share the results of [a] search or even sell it," ante at ___ (slip op. at 57); his phone was a smartphone; his smartphone had GPS functionality; his smartphone had Google's operating system or a downloaded Google application with enabled location-tracking services; he had that particular phone with him at the time of the robbery; and he was logged into his Google account on that smartphone at the time of the robbery. Maybe all of 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 State v. Irelan, 375 N.J. Super. 100, 118 (App. Div. 2005)).

Because the certification the detective submitted in support of the application for Warrant I did not contain facts sufficient to support a finding of probable cause, Warrant I was invalid. And our inquiry should end there.

For the majority, the detective's unsupported assertions about most people possessing cell phones and most people carrying them with them is enough to establish probable cause. See ante at ___ (slip op. at 45) ("Given the recognized widespread use of cell phones and the unavailability of public phones, the State is correct that it need not have to prove defendant was using a cell phone in order to establish probable cause . . . ."). That is a leap too far for me. Under that standard – most people have phones and most people carry them – warrants to Google would be issued in every single criminal case. If that's not a general warrant, what is? If we accept that standard, Google, and every other cell-phone service provider, effectively would be turned into an arm of law enforcement.

The majority "find[s] no clear guidance in the federal law." Ante at ___ (slip op. at 25). But New Jersey Supreme Court precedent, as cited by the motion judge, regarding the protections provided under New Jersey's Constitution is clear: our State Constitution affords "individuals a reasonable expectation of privacy in their cell-phone location information." State v. Manning, 240 N.J. 308, 330 (2020) (citing State v. Earls, 214 N.J. 564, 588 (2013)).

The County Prosecutors Association of New Jersey, as amicus curiae, asserts the "use of technology is a compromise: for every advantage reaped, a

price is owed," the price "often" being the "forfeiture" of an individual's privacy rights. To the contrary, technological developments require courts to be ever vigilant in protecting the privacy rights of our citizens:

> As Justice Brandeis explained in his famous dissent, the Court is obligated—as "[s]ubtler 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. Olmstead v. United States, 277 U.S. 438, 473-474 (1928). Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers, "after consulting the lessons of history," drafted the Fourth Amendment to prevent.
>
> [Carpenter v. United States, 585 U.S. 296, 320 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).]

But we need not tackle in this case the potentially wide-sweeping implications of geofence warrants. And contrary to how the majority characterizes this dissent, ante at ___ (slip op. at 48), I express no broad view about what police must do to gain access to cellular-technology-based information. Taking it one step at a time, as we should and must under our well-settled law, we need to decide as a threshold matter if the finding of probable cause for the issuance of Warrant I was supported by adequate facts. Because the facts set forth in the detective's certification were not sufficient to support a

finding of probable cause, we should affirm the order granting defendant's suppression motion.

For these reasons, I respectfully dissent.