

2025 PA Super 209

COMMONWEALTH OF PENNSYLVANIA	:	IN THE SUPERIOR COURT OF
	:	PENNSYLVANIA
	:	
v.	:	
	:	
	:	
KEITH ANTHONY CHOICE	:	
	:	
Appellant	:	No. 1252 EDA 2024

Appeal from the Judgment of Sentence Entered April 9, 2024
In the Court of Common Pleas of Montgomery County Criminal Division
at No(s): CP-46-CR-0001125-2022

BEFORE: MURRAY, J., McLAUGHLIN, J., and FORD ELLIOTT, P.J.E.*

OPINION BY MURRAY, J.:

FILED SEPTEMBER 18, 2025

Keith Anthony Choice (Appellant) appeals from the judgment of sentence imposed following his nonjury conviction of aggravated assault.¹ In this matter of first impression, Appellant challenges the search warrants securing from Google, LLC (Google), *inter alia*, the location history (LH) data from cellular devices present at the time and place of the crime (a process known as “geofencing”).² After careful review, we affirm.

* Retired Senior Judge assigned to the Superior Court.

¹ 18 Pa.C.S.A. § 2702(a)(4).

² As described further, *infra*,

[un]like a warrant authorizing surveillance of a known suspect, geofencing is a technique law enforcement has increasingly utilized when the crime location is known but the identities of
(Footnote Continued Next Page)

The trial court summarized the facts underlying this appeal:

At approximately 9:58 p.m. on [] January 23, 2019, [Pennsylvania State Police (PSP) troopers] responded to a call into [the] Montgomery County 911 dispatch center of a possible shooting on northbound State Route 309 (“[Route] 309”). The troopers were dispatched to the Fort Washington Toll Plaza on the Pennsylvania Turnpike, Upper Dublin Township in Montgomery County. There they met with [the victim, John Cramer (Cramer),] and Upper Dublin Township [police] officers who were securing the scene while [emergency medical services (EMS) personnel] provided aid[. EMS personnel] determined that Cramer had a graze wound on his upper right arm[,] after having been shot with a firearm. When Cramer exited his silver 2014 Toyota Tundra [(Tundra)], a single copper-jacketed bullet fell to the ground and was recovered by a [t]rooper. ([Search Warrant] Affidavit of Probable Cause presented to the Honorable William R. Carpenter[(Judge Carpenter)³], Montgomery County Court of Common Pleas, on 12/8/20, at 1, Commonwealth Exhibit C-1 (“[Exhibit] C-1” [or “the December 2020 search warrant”])).

... Trooper Eugene J. Tray [(Trooper Tray)] was assigned as the primary investigator [after] the [Upper Dublin Township Police Department] requested [the PSP] to assume the primary role in this investigation.

Suppression Court Opinion, 1/2/25, at 2-3 (footnote added).

suspects are not. Thus, geofence warrants effectively work in reverse from traditional search warrants. In requesting a geofence warrant, law enforcement simply specifies a location and period of time, and, after judicial approval, companies conduct sweeping searches of their location databases and provide a list of cell phones and affiliated users found at or near a specific area during a given timeframe, both defined by law enforcement.

United Stated v. Smith, 110 F.4th 817, 822 (5th Cir. 2024) (quotation marks, brackets, and citations omitted).

³ Judge Carpenter authorized each of the search warrants relevant to this appeal. The Honorable Thomas P. Rogers presided over Appellant’s relevant court proceedings.

At 12:10 a.m., on January 24, 2019, Trooper Tray interviewed Cramer at the Abington Hospital, where Cramer was receiving treatment. Cramer related the following to Trooper Tray, as described by the trial court:

Cramer was employed as a licensed practical nurse ... in Wyncote, Montgomery County[, on the date of the incident]. At approximately [8]:30 p.m., [Cramer] left work in his [Tundra], stopped briefly at a friend's house, and then drove to the Wawa [convenience store] located on Limekiln Pike in Cheltenham. After approximately twenty (20) minutes, Cramer left the Wawa parking lot, turned left and entered ... [Route 309] northbound on his way to the Turnpike, and then home.

Cramer continued northbound on [Route] 309 traveling at approximately 60 miles per hour in the left-hand lane. Around the time when Cramer observed the PA Turnpike $\frac{3}{4}$ [m]ile [n]orthbound road sign, he made a lane change into the right-hand lane.

Immediately after completing the lane change, Cramer heard a "pop" or "bang" sound and then felt a pain in his right arm. At the same time, his nose began to bleed[,] and his [Tundra's] front passenger-side window went down, even though he had not pushed the window button. Cramer attempted to put the window back up but was unable to do so. He also felt his right arm and believed that he may have been shot.

At about this same time, Cramer noticed a maroon, dark-colored vehicle[(the maroon vehicle)], with a possible New Jersey registration, pull directly out in front of his [Tundra] after passing him on the right shoulder. Cramer could see two silhouettes of people seated inside of the maroon vehicle that he described as older and having a "box shape[.]" The maroon vehicle then accelerated rapidly ahead, with Cramer attempting to follow.

As Cramer was following the maroon vehicle attempting to ascertain the registration plate, he called 911 from his cell phone. He proceeded to follow the [maroon] vehicle for over a mile, past the Turnpike exit (mile marker 4.6), before the [maroon] vehicle exited [Route] 309. Cramer believed it was the [] exit ... for ... Highland Avenue. At the bottom of the ramp, the maroon vehicle made a right-hand turn, at which point Cramer lost sight of [it].

After losing sight of the maroon vehicle, Cramer made a U-turn and traveled back on southbound [Route] 309 to the Turnpike interchange before coming to a stop at the PA Turnpike building at the Fort Washington interchange, where he remained until law enforcement and EMS personnel arrived.

Id. at 4-5 (paragraph designations omitted) (citing Exhibit C-1 at 3).

The next morning, following his interview with Cramer, Trooper Tray spoke with an individual (the witness)⁴ who disclosed the following:

[The witness] ... heard on the local news that a shooting occurred on [Route] 309 [n]orthbound just prior to the Turnpike exits. [The witness] stated that he was driving home at [the time of the shooting] and recalled that he observed [a vehicle, matching the description of Cramer's Tundra], traveling northbound in the left lane of travel for an extended period of time. The [] Tundra then changed lanes to the right, forcing a vehicle to the right of the [Tundra] onto the right shoulder. [The witness] could describe[] this vehicle only as a "dark sedan." Immediately after witnessing the unsafe lane change, [the witness] heard a "punk" sound and the dark sedan passed the [Tundra] on the right.

Exhibit C-1 at 4.

After conducting additional investigation not relevant to this appeal, Trooper Tray applied for the December 2020 search warrant, seeking solely LH "data"⁵ generated from devices [] report[ing] a location with a geographical

⁴ The record does not disclose the identity of the witness.

⁵ One commentator has observed that law enforcement has increasingly sought LH data in criminal investigations. **See** Barbara Bathke, *Google and the Role of Surveillance Intermediaries in Geofence Warrants*, 26 TUL. J. TECH. & INTELL. PROP. 111, 118 (2024) (noting that Google received "approximately 20,000 geofence warrant requests for [LH] data between 2018 and 2020." (footnote omitted)).
(Footnote Continued Next Page)

region bounded” by latitude/longitude coordinates, and within dates and times, set forth in the affidavit. Exhibit C-1 at 1 (footnote added).^{6, 7}

LH data is highly sought after by law enforcement. Agencies use legal processes like search warrants, court orders, and subpoenas to compel the production of data. Typically, through these procedures, police can request access to a broad range of data taken from Google devices and accounts. Geofence warrants, however, are unique. The information sought after is not tied to a specific person, account, or device. LH is the only type of location data that is not stored in association with a specific Google account. Further, it is the only type of location data stored at a level of precision sufficient to be searched and produced in response to a geofence warrant. Location data taken from Google search engine searches, for example, is not stored with sufficient locational specificity. As a result, LH emerges as highly sought after evidence in the course of criminal investigations.

Id. at 116 (footnotes and quotation marks omitted).

⁶ Significantly, the December 2020 search warrant limited its search request to LH data, and **not** the contents of any cellular devices (device IDs) within the described geographical coordinates. As explained further *infra*, upon execution of a search warrant, Google initially anonymizes the device IDs falling within the particular date, time, and latitude/longitude parameters requested in the warrant, in order to safeguard the privacy of any users whose device IDs law enforcement determine are irrelevant to its investigation.

⁷ At the suppression hearing, Trooper Tray testified that, on March 2, 2020, he secured two search warrants (the March 2020 search warrants) for LH data from Google. N.T. (Suppression Hearing), 10/5/23, at 26. The March 2020 search warrants sought LH data from different target locations. **Id.** Trooper Tray explained that “because Google had changed their policy for how they wanted to respond to law enforcement requests[,]” he secured the December 2020 search warrant, combining LH data sought from both locations into a single warrant application. **Id.** The December 2020 search warrant contains the same information and search parameters as the March 2020 search warrants.

Pertinently, in addition to including the above facts, Trooper Tray detailed therein the content of Cramer's call to 911:

During the 911 call, Cramer mentions both the PA Turnpike ½ mile road sign and the PA Turnpike ¾ mile road sign, when trying to describe to dispatchers where the shooting took place. Based on the information obtained from this call, [Cramer's] statements to investigators and the statement from [the w]itness [], it is probable the shooting occurred in a portion of [Route] 309 northbound at or near these two road signs. The Turnpike road signs are located at mile markers 3.1 ([¾] mile road sign) and 3.6 ([½] mile road sign), respectively. Cramer's 911 call was received [by] Montgomery County 911 at exactly 21:23:58 hours on 01/23/19. Twelve seconds after the call is received by 911, Cramer tries to describe his current location by stating that he is passing the "Highland Avenue ¼ mile" road sign (mile marker 5.1). Then, at 21:25:18 hours (after briefly losing cellular connection with 911), Cramer tells dispatchers that he lost sight of the [maroon] vehicle and "turned around." It is known from [Cramer's] in-person statement made to investigators[] that Cramer turned around at the Highland Avenue exit and proceeded south to the Turnpike interchange[,], where he awaited police response.

Exhibit C-1 at 5 (capitalization modified).

In the December 2020 search warrant, Trooper Tray averred that, based on his

knowledge, training and experience as a law enforcement officer, I am aware that the use of handheld cellular devices has become prevalent by most members of society. In addition, I have investigated many incidents in which I was able to determine that the perpetrators of crimes have been in possession of a handheld cellular device during the commission of the crime. It is a reasonable conclusion that the perpetrator(s) of the attempted homicide on [Route] 309 northbound on 01/23/19 was in possession of a handheld, cellular device during the commission of the crime.

Id. at 6 (capitalization modified).

The warrant application identified Google as “an internet company and provider of electronic communication services[,]” and set forth the following:

- [] Google[] is the developer of the Android mobile operating system. **Greater than 50% of all cellular devices in the United States operate on the Android system.**
- These Android-based devices prompt the user to add a Google account to their device upon initial activation of the device.
- Google[] collects and retains [LH] data from Android-based mobile devices when a Google account user has enabled Google location services. Google[] uses this information for location-based advertising, location-based search results, and other location-based services which they provide to their users.
- The location information is derived from a variety of sources, including Global Position[ing] System (GPS) data, cell site/cell tower information, and WiFi access points, among other sources of location data.
- This information is collected by Google[] in the background, meaning that no[]user[-]initiated activity is necessary for the collection of such data.
- Subsequently, this location information concerning an Android-based cellular device can identify the specific geographic location of the device even during times when it was not in active use.
- Additionally, such location information is connected to other data retained by Google[,] which would assist in identifying the device and the subscriber/user of the said device.
- It is more likely than not that the cellular telephones possessed by the actor(s) responsible for this attempted homicide are Android-based devices. It is similarly likely that Google[] possesses and retains the [LH] data and information identifying the subscriber/user of such devices.
- Finally, it is more likely than not that other individuals within the target locations on the date and time of the attempted homicide were in possession of their respective cellular

telephones, that such cellular devices were Android-based, and that such other individuals are potential witnesses to the crime. It is similarly likely that Google[] possesses and retains the [LH] data and information identifying the subscriber/user of such devices.

Id. at 6 (capitalization modified; emphasis added). In the affidavit, Trooper Tray further averred that Route “309 and the surrounding local roads are sparsely traveled at the time of day requested by this legal process. Therefore, it is unlikely that a vast number of vehicles containing [device IDs] will be located within either search parameters.” **Id.** at 5.

Based upon the foregoing, the December 2020 search warrant sought an anonymized list of “information specifying the corresponding unique [device ID], timestamp, coordinates, display radius and data source” (anonymized list), using LH data queried within the following parameters:

1. [] Route 309 northbound from mile marker 3.1 to mile marker 3.8 (Springfield Township and Whitemarsh Township, Montgomery County, PA) from 21:20:00 hours to 21:27:00 hours on January 23, 2019[;]
2. Highland Avenue exit ramp and surrounding areas (Upper Dublin Township, Montgomery County, PA) from 21:20:00 hours to 21:27:00 hours on January 23, 2019[.]

Id. at 5, 8-9 (capitalization modified); **see also id.** (explaining that “[t]he two polygon target locations ... represent a roughly rectangular shape covering the two (2) specified locations”); **id.** at 8-9 (delineating the latitude/longitude points defining the target locations).

Finally, the December 2020 search warrant outlined the next step in the investigative process, whereby, upon receipt of the anonymized list,

law enforcement shall review the anonymized list to remove devices that are not relevant to the investigation, for example, devices that were not in the location for a sufficient period of time. If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the time period that falls outside [the] target location. These contextual location coordinates may assist law enforcement in identifying devices that were outside of the target location, were not within the target location for a long enough period of time, were moving through the target location in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

Id. at 8, 9 (capitalization modified).

After execution of the December 2020 search warrant, on February 9, 2021, Trooper Tray received email correspondence from Google's "law enforcement portal" providing the requested anonymized list of device IDs. N.T., 10/5/23, at 10. At the suppression hearing, Trooper Tray testified that he identified **only one device ID** within the anonymized list that was relevant to his investigation. ***Id.*** at 11. Trooper Tray explained that, upon his request, Google "provided more descriptive location information for that particular device that I found to be pertinent to my investigation." ***Id.*** at 12.

On February 16, 2021, utilizing the anonymized information provided by Google, Trooper Tray prepared a second search warrant, admitted into evidence at the suppression hearing as Commonwealth Exhibit C-2 (Exhibit C-2 or the February 2021 search warrant), seeking the identity of "the user or subscriber of that particular device ID." ***Id.*** at 12. On November 3, 2021, Google responded to the February 2021 search warrant by providing Trooper

Tray with a “one-page subscriber identity document that stated the G[]mail account associated with that device ID, a phone number associated with the device ID, and a name and a date of birth inputted by the user at the time of their Google account creation[.]” ***Id.*** at 13. Using this deanonymized information, Trooper Tray conducted additional investigation⁸ that led him to charge Appellant with terroristic threats⁹ and aggravated assault.

On April 3, 2023, Appellant filed a counseled suppression motion,¹⁰ challenging the “geofence searches performed pursuant to the respective warrants” as overbroad and lacking in “particularized probable cause to search each of the millions of user accounts searched.” Suppression Motion, 4/3/23, ¶ 8. On July 31, 2023, Appellant filed an amended suppression motion advancing the same arguments. ***See generally*** Amended Suppression

⁸ Trooper Tray’s incident report, entered into evidence at the October 5, 2023, suppression hearing as Appellant’s Exhibit D-7 (Exhibit D-7), discloses that law enforcement seized as evidence Appellant’s “iPhone in a black case[.]” Exhibit D-7 at 26 (capitalization modified). By way of context,

[LH] data is extracted from Google’s many applications that track user locations, including Gmail, Google Chrome, Google Maps, and Google Docs. While other cell phones like Apple iPhones do not gather location data in the same way [as Android devices], these phones often utilize Google applications that collect location datapoints.

Bathke, supra, at 114 (footnotes omitted).

⁹ 18 Pa.C.S.A. § 2706(a)(1).

¹⁰ On June 28, 2022, Appellant filed an omnibus pretrial motion, which made boilerplate assertions inapplicable to the instant factual circumstances.

Motion, 7/31/23. On August 8, 2023, Appellant filed a second amended suppression motion, again advancing the same arguments, and appending a “declaration” authored by Google policy specialist Mitchell Wootten (Wootten). **See** Second Amended Suppression Motion, 8/8/23, Exhibit A.

The Commonwealth filed an answer arguing that “the Google [g]eofence inquiry is not a search, [Appellant] does[not] have standing to challenge the inquiry, and thus the [suppression c]ourt should never get to the issue of whether individualized probable cause is required.” Answer, 8/28/23, ¶ 3.

The matter proceeded to a suppression hearing on October 5, 2023. The Commonwealth called as its only witness Trooper Tray, and offered as evidence, without objection, Exhibits C-1 and C-2. The Commonwealth also offered as evidence, without objection, Google’s terms of service, effective October 25, 2017, and January 5, 2022, as Exhibits C-3 and C-4, respectively.

Appellant presented the testimony of Wootten, and presented, without objection, Wootten’s declaration as Defense Exhibit D-7 (Exhibit D-7), and documents titled “Google Privacy & Terms,” explaining how Google retains data and uses location information, as Exhibits D-8 and D-9, respectively. Wootten explained that Google offers LH “as a service,” and that LH data is stored in a “common [LH] database.” N.T., 10/5/23, at 35; **see also** Exhibit D-7, ¶ 3 (stating, “Google LH is 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[,]” and that “[u]sers must explicitly opt in

to [LH services]."); Exhibit C-3 at 9 (unpaginated) ("[Google] collect[s] information about the app[lications], browsers, and devices you use to access Google services[.]").¹¹ Wootten testified that Google users retain the ability to "edit, review, and delete their [LH data] with [Google]." **Id.** According to Wootten, Google "requires a search warrant [for the disclosure of LH data]." **Id.** at 36. Wootten testified that approximately "one-third of Google users" opt-in to LH services, which amounts to "[r]oughly tens of millions" of users. **Id.** at 37.

Wootten next described the three-step process "that Google uses when it [responds to] a geofence warrant":

The first step of the geofence process, whenever law enforcement submits a [search warrant] to us, we take it, we analyze it, we pack it, extract the data, and then package it together, and submit it. [**We a**nonymize the data]¹² and then submit it back over to

¹¹ Neither Appellant nor the Commonwealth presented any evidence as to the manner in which Google users "explicitly opt in" to LH services.

¹² In general, Exhibit D-9 explains,

Google uses anonymized and pseudonymized location information to help enhance people's privacy. Anonymized information generally cannot be associated with any individual. Pseudonymized information may be tied to a unique identifier, such as a string of numbers, rather than more personally identifiable information such as a person's account, name, or email address. Anonymized and pseudonymized location information may be used by Google in its products and services for purposes such as advertising or trends.

Exhibit D-9 at 10.

law enforcement through our law enforcement respondent coordinator[(Step 1)].

....

The next step is Step 2, and this is additional contextual [LH] data. **This is data that is anonymized still**, and it just provides a little more context¹³ to the original Step 1 data[(Step 2)].

The third step is when we actually unmask and identify this data and produce that to law enforcement[(Step 3)].

Id. at 37-38 (some paragraph breaks omitted; footnotes and emphasis added); **see also** Exhibit D-7, ¶¶ 7-14 (detailing the foregoing three-step process).¹⁴ Discussing Step One, concerning the accuracy of the display radius generated after inputting the latitude/longitude coordinates, Wootten

¹³ In his declaration, Wootten explained, "This additional contextual LH information can assist law enforcement in eliminating devices in the production that were not in the target location for enough time to be of interest, were moving through the target location in a manner inconsistent with the evidence, or otherwise are not relevant to the investigation." Exhibit D-7, ¶ 13.

¹⁴ Throughout his brief, Appellant alternatively refers to a "warrant" and "warrants" in arguing his claims. Although Appellant does not specifically refer to the February 2021 search warrant, he indicates that the warrants were executed in three steps. While not clearly delineated in his brief, we discern that Appellant refers to the three steps set forth in Wootten's testimony and declaration. Instantly, Steps One and Two are detailed in the December 2020 search warrant, and Step Three is set forth in the February 2021 search warrant. **See** Exhibit C-1 at 8-9; Exhibit C-2 at 10.

explained that “Google’s goal is to have a 68 percent confidence and chance that the [device ID] will be within the map’s display radius.” **Id.** at 41.¹⁵

At the conclusion of the hearing, the suppression court took the matter under advisement. On March 25, 2024, the suppression court filed findings of fact and conclusions of law (FFCL), and an order denying Appellant’s suppression motion. The suppression court opined that, because the Commonwealth secured a search warrant, it was not required to “decide whether a geofence inquiry is a search and, thus, requires a warrant.” FFCL, 3/25/24, at 26. The suppression court determined, however, that “the warrants issued in this case were both supported by probable cause and [] model[s] of particularity” **Id.** (quotation marks omitted).

¹⁵ In Exhibit D-7, Wootten represented that

LH records are deemed responsive to a geofence warrant (*i.e.*, a user’s estimated location is treated as falling within the scope of the warrant) if the stored latitude/longitude coordinates fall within the search area described in the warrant. Each set of coordinates saved to a user’s LH include a display radius value, measured in meters, that reflects Google’s confidence in the saved coordinates. Google’s goal is that there will be a 68% chance that the user is actually within the display radius. A set of coordinates that falls within the search area described in a geofence warrant is deemed responsive even if some portion of the corresponding display radius falls outside of the search area.

Exhibit D-7, ¶ 10.

On March 27, 2024, the matter proceeded to a stipulated bench trial, after which the trial court convicted Appellant of the above-described charge.¹⁶ On April 9, 2024, the trial court sentenced Appellant to 6 to 23 months' incarceration, followed by two years' probation. Appellant filed a timely notice of appeal. Both the trial court and Appellant have complied with Pa.R.A.P. 1925.

Appellant raises the following two issues:

- I. Did the [suppression] court err in failing to grant [Appellant's] motion to suppress[,] pursuant to Article 1, § 8 of the Pennsylvania Constitution and the 4th Amendment of the United States Constitution[,] on the ground that the search warrant in question and affidavit of probable cause failed to establish individualized probable cause that the shooter possessed a cell phone, let alone an Android[-]based device?
- II. Did the [suppression] court err in failing to grant [Appellant's] motion to suppress[,] pursuant to Article 1, § 8 of the Pennsylvania Constitution and the 4th Amendment of the United States Constitution[,] on the ground that each of the three steps in the geofence process articulated in the search warrant in question and accompanying affidavit of probable cause and carried out by Google pursuant to the warrant, constituted an unconstitutionally overbroad search that also lacked particularity of probable cause and that recovered constitutionally protected location history data?

Appellant's Brief at 3.¹⁷

¹⁶ The Commonwealth withdrew Appellant's terroristic threats charge prior to trial.

¹⁷ The Commonwealth argues that Google LH data is not constitutionally protected information. **See** Commonwealth Brief at 15. However, consistent with the doctrine of constitutional avoidance, because we conclude that the
(Footnote Continued Next Page)

Appellant challenges the denial of his suppression motion. “Our standard of review in addressing a challenge to the denial of a suppression motion is limited to determining whether the suppression court’s factual

geofence warrants obtained by the Commonwealth in the instant case were sufficiently particular and not overbroad, we decline to decide this issue. **See Commonwealth v. Collins**, 286 A.3d 767, 773 (Pa. Super. 2022) (observing that “we ought not to pass on questions of constitutionality ... unless such adjudication is unavoidable.” (quoting **Spector Motor Serv. v. McLaughlin**, 323 U.S. 101, 105 (1944))); **see also Commonwealth v. Dunkins**, 263 A.3d 247, 253 n.5 (Pa. 2021) (“It has long been [a] considered practice not to decide ... any constitutional question in advance of the necessity for its decision[.]” (citation omitted)); **Commonwealth v. Homoki**, 621 A.2d 136, 140 (Pa. Super. 1993) (“We will not attempt to resolve constitutional issues unless the specific issue is before us[,] and the resolution of the issue is **absolutely necessary** to the decision of the case.” (emphasis added; citation omitted)). **But see Allegheny Reprod. Health Ctr. v. Pennsylvania Dep’t of Human Servs.**, 309 A.3d 808, 912 (Pa. 2024) (concluding the doctrine of constitutional avoidance did not apply when considering two issues concerning constitutional rights, where, *inter alia*, “[t]he constitutional question **will not be avoided by the proposed remand**.” (emphasis added)). As we can resolve Appellant’s issues on narrower grounds than proposed by the Commonwealth, we do so herein.

Moreover, the record before us (which does not include, *e.g.*, an explanation of how Google users “opt-in” to LH services) is ill-suited for the disposition of whether LH data is constitutionally protected information. **See Commonwealth v. Skipper**, 277 A.3d 617, 620 (Pa. Super. 2022) (“[B]efore [a] defendant must prove [a] privacy interest in [an] area searched, [the] Commonwealth must initially satisfy its burden of production by presenting evidence showing [the] defendant lacked any protected privacy interest[.]” (emphasis omitted) (citing **Commonwealth v. Enimpah**, 106 A.3d 695, 700-01 (Pa. 2014))).

Finally, we note that a closely related issue is currently pending before our Supreme Court. **See Commonwealth v. Kurtz**, 306 A.3d 1287 (Pa. 2023) (granting *allocatur* to decide, *inter alia*, “whether the Superior Court erred in concluding that an individual does not have a reasonable expectation of privacy in his or her electronic content, particularly in his or her private internet search queries and IP address?”).

findings are supported by the record and whether the legal conclusions drawn from those facts are correct.” **Commonwealth v. Dewald**, 317 A.3d 1020, 1030 (Pa. Super. 2024) (citation and brackets omitted). “We are bound by the facts found by the trial court so long as they are supported by the record, but we review its legal conclusions *de novo*.” **Commonwealth v. Rivera**, 316 A.3d 1026, 1031 (Pa. Super. 2024) (citation omitted). “Our scope of review from a suppression ruling is limited to the evidentiary record that was created at the suppression hearing.” **Commonwealth v. Tillery**, 249 A.3d 278, 281 (Pa. Super. 2021) (citations omitted).

“Where, as here, the defendant is appealing the ruling of the suppression court, we may consider only the evidence of the Commonwealth and so much of the evidence for the defense as remains uncontradicted.” **Commonwealth v. Yandamuri**, 159 A.3d 503, 516 (Pa. 2017) (citation omitted). “[I]t is within the suppression court’s sole province as factfinder to pass on the credibility of witnesses and the weight to be given their testimony.” **Commonwealth v. Ochoa**, 304 A.3d 390, 396 (Pa. Super. 2023) (citation and brackets omitted). “The suppression court is free to believe all, some or none of the evidence presented at the suppression hearing.” **Commonwealth v. Byrd**, 185 A.3d 1015, 1019 (Pa. Super. 2018) (citation omitted).

Further, where a defendant files a suppression motion, “[t]he Commonwealth shall have the burden of going forward with the evidence and

of establishing that the challenged evidence was not obtained in violation of the defendant's rights." Pa.R.Crim.P. 581(H); **see also id.**, Comment (stating that the standard of proof is a preponderance of the evidence).

Appellant first argues, citing **Commonwealth v. Jacoby**, 170 A.3d 1065 (Pa. 2017), and **Commonwealth v. Ani**, 293 A.3d 704 (Pa. Super. 2023) (both discussed *infra*), that the December 2020 search warrant

fail[s] to set forth probable cause to search Google's [LH] database[,] since [it] fail[s] to articulate a single individualized fact that [Appellant] possessed a cell phone during the shooting, let alone that the phone was based on an Android operating system and that location services had been enabled.

Appellant's Brief at 21-22.

Appellant claims that the averments in the December 2020 search warrant concerning the ubiquity of cell phone usage and the likelihood that Google possessed information relevant to the instant offense

are the exact sort of categorical assumptions that **Jacoby, supra**, and **Ani, supra**[,] have found to be insufficient to establish probable cause. None of them pertain to the actual suspect in the instant case. There are no facts cited which indicate that the shooter possessed a cell phone, let alone an Android phone for which location services had been enabled.

Appellant's Brief at 21.

In response, the Commonwealth argues that **Jacoby** and **Ani** are distinguishable:

Here, the police were not seeking [] private information regarding any specific individual. Instead, the police had probable cause to believe that the shooter was at a particular place at a particular time[,] and the police sought information from Google to identify

possible suspects based on Google user [LH] information for the relevant time and place.

The police cannot rely on general assumptions without facts to search an individual's property where they lack the factual nexus to do so. ... Here, the police were able to articulate where they believed the crime occurred, when they believed the crime occurred, and why, based on the ubiquitous nature of cell[]phones and Google features on devices, they believed that evidence of the crime at issue would probably be found in Google's records.

Commonwealth Brief at 32-33.

Relying on this Court's decision in ***Commonwealth v. Kurtz***, 294 A.3d 509 (Pa. Super. 2023), ***appeal granted***, 306 A.3d 1287 (Pa. 2023), the Commonwealth maintains that

[i]t was not necessary for the Commonwealth ... to lay out only "concrete evidence" that established the shooter used a Google device or feature before a search warrant could be issued. ... [T]he proper question to ask here is whether the search warrants set forth ground to show a "fair probability" that the Google [LH data] being sought ... would uncover evidence related to the shooting at issue.

Id. at 33-34.

In his related second issue, Appellant argues the geofence search warrants ran afoul of "the test for particularity of probable cause" and "the test for overbreadth[.]" Appellant's Brief at 35. Appellant points out that Step One of the geofence process "authorize[d] a search of tens of millions of [LH] accounts with no relation to the crime whatsoever." ***Id.*** at 34. Appellant argues that, "[i]n light of th[e] vast discrepancy between the number of items for which probable cause existed and the numbers of items to be searched

pursuant to the warrant, the warrants in question simply cannot survive the test for particularity ...[,] as well as the test for overbreadth” **Id.** at 35; **see also id.** at 36 (arguing that “since the results of the search have only 68% accuracy, a distinct possibility exists that Google users with no connection to the geofence area could be subjected to the search.”).

Appellant further argues that Step Two, which “permits the investigating officer to request additional data for every phone found to be within the geofence boundaries – including additional data that is outside the boundaries ... contains no objective standards by which such selection is to be guided.” **Id.** at 37-38. Appellant maintains that Steps Two and Three gave law enforcement “constitutionally infirm,” “unbridled discretion in narrowing the initial list of [device IDs] identified by Google.” **Id.** at 43. Rather, Appellant argues, the geofence boundaries “entailed a populous suburban area with a large number of private residences that had no connection to the crime and for which no particularized probable cause existed.” **Id.** at 44.

As there are no Pennsylvania decisions resolving this issue, in support of his second argument, Appellant cites cases from other jurisdictions finding the geofence process to be constitutionally infirm. **See Smith**, 110 F.4th at 837 (“[T]he quintessential problem with [Step One of] 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.” (emphasis in original; footnote omitted));

United States v. Chatrie, 590 F.Supp.3d 901, 929 (E.D. Va. 2022) (concluding the government’s geofence warrant lacked particularized probable cause where, *inter alia*, the warrant “sought location information for *all* Google account owners who entered the geofence over the span of an hour.” (emphasis in original)), **affirmed by**, 107 F.4th 319 (4th Cir. 2024), **reh’g en banc granted**, 136 F.4th 100 (4th Cir. 2025) (affirming the judgment of the district court, *per curiam*, in a fractured opinion consisting of eight concurrences and a dissent); **Matter of Search of Info. Stored at Premises Controlled by Google**, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (stating that a warrant’s particularity requirement “leaves the executing officer with no discretion as to what to seize, but the warrant here gives the executing officer unbridled discretion as to what device IDs would be used as the basis for the mere formality of a subpoena to yield the identifying subscriber information[.]” (citation omitted)); **People v. Meza**, 90 Cal. App. 5th 520, 538, 540 (2023) (finding, *inter alia*, the geofence warrant at issue was overbroad, because (1) it “authorized the identification of any individual within six large search areas without any particularized probable cause to each person or their location”; and (2) the time frame sought began ninety minutes before the suspects were seen at the relevant target location).¹⁸

¹⁸ We may consider the decisions of federal courts and courts of other jurisdictions for their persuasive value:

(Footnote Continued Next Page)

The Commonwealth disputes Appellant's claim that the geofence process grants law enforcement "unbridled discretion" to review the personal information of uninvolved third parties:

Here, [] using the geofence process, the government does not actually conduct the search. The government does not see personal information of non-pertinent individuals. And, the government does not take possession of or have access to the data regarding any Google subscriber or user, aside from the narrow information described with particularity about the presence of a Google device or user at a particular time and in a particular place.

Commonwealth Brief at 39.

The Commonwealth maintains that the search warrant affidavits "detailed the thorough investigation conducted by the PSP which enabled them to specify the very precise locations and very narrow time period that applied to their search." *Id.* The Commonwealth emphasizes that "[t]he government did not track the movements of [A]ppellant. The government did not gain

Our law clearly states that, absent a United States Supreme Court pronouncement, the decisions of federal courts are not binding on Pennsylvania state courts, even when a federal question is involved

Further: When confronted with a question heretofore unaddressed by the courts of this Commonwealth, we may turn to the courts of other jurisdictions. Although we are not bound by those decisions, we may use decisions from other jurisdictions for guidance to the degree we find them useful and not incompatible with Pennsylvania law.

Commonwealth v. McIntyre, 333 A.3d 417, 428 (Pa. Super. 2025) (quotation marks and citations omitted).

access to any other information that Google collected from [A]ppellant concerning anything other than his presence at the given location at the given time.” **Id.**

Having outlined the parties’ positions, we turn to the applicable law.

“The Fourth Amendment of the United States Constitution and Article 1, Section 8 of the Pennsylvania Constitution protect against unreasonable searches and seizures.” **Commonwealth v. Adorno**, 291 A.3d 412, 415-16 (Pa. Super. 2023); **see** U.S. CONST. AMEND. IV (“[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.”); PA. CONST. art. I, § 8 (“[N]o warrant to search any place or to seize any person or things shall issue without describing them as nearly as may be, nor without probable cause, supported by oath or affirmation subscribed to by the affiant.”).

The purpose of the Fourth Amendment is to prevent general (*i.e.*, overbroad) searches and to “ensure[] that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.” **Commonwealth v. Turpin**, 216 A.3d 1055, 1063-64 (Pa. 2019); **see also id.** at 1066 (observing “‘as nearly as may be’ language of Article I, Section 8 [] require[s] more specificity in description of items to be seized than federal particularity requirement” (citation omitted)). Pennsylvania’s stricter specificity

requirement “makes general searches impossible and prevents the seizure of one thing under a warrant describing another.” **Id.** at 1066.

Consequently, a warrant must describe with sufficient particularity the person or property to be searched, and must not be sought for the purpose of generally “rummaging” through an individual’s possessions. **Commonwealth v. Young**, 287 A.3d 907, 920 (Pa. Super. 2022). Moreover, “all warrants, be they for the search of physical or digital spaces, must (1) describe the place to be searched and the items to be seized with specificity[,] and (2) be supported by probable cause to believe that the items sought will provide evidence of a crime.” **Id.** at 921 (quotation marks and citation omitted).

Pennsylvania Rule of Criminal Procedure 203(D) provides that, “[a]t any hearing on a motion for the ... suppression of evidence ... obtained pursuant to a search warrant, no evidence shall be admissible to establish probable cause other than the affidavits [sworn to before the issuing authority].” Pa.R.Crim.P. 203(D); **Commonwealth v. Shackelford**, 293 A.3d 692, 698 (Pa. Super. 2023) (“Our review of a challenge to a search warrant based on an affidavit of probable cause is limited to the information within the four corners of the affidavit.” (citations omitted)); **id.** (“[A] reviewing court may not conduct a *de novo* review of the issuing authority’s probable cause determination but, instead, is tasked simply with the duty of ensuring the issuing authority had a substantial basis for concluding that probable cause existed.” (quotation marks and citations omitted)).

“The linch[.]pin that has been developed to determine whether it is appropriate to issue a search warrant is the test of probable cause.”

Commonwealth v. Davis, 241 A.3d 1160, 1173 (Pa. Super. 2020) (citation omitted).

The existence of probable cause is measured by examining the totality of the circumstances. Probable cause exists where the facts and circumstances within the affiant’s knowledge and of which he or she has reasonably trustworthy information are sufficient in and of themselves to warrant a person of reasonable caution in the belief that a search should be conducted. [**The issuing authority**], **when deciding whether to issue a search warrant, must make a practical, common-sense decision whether, given all of the circumstances set forth in the affidavit** ... including the veracity and basis of knowledge of persons supplying hearsay information, **there is a fair probability that contraband or evidence of a crime will be found in a particular place**. Conversely, a court reviewing a search warrant determines only if a substantial basis existed for the magistrate to find probable cause.

Commonwealth v. Kimmel, 331 A.3d 26, 30 (Pa. Super. 2025) (emphasis added) (quoting ***Jacoby***, 179 A.3d at 1080-81); **see also *Illinois v. Gates***, 462 U.S. 213, 236 (1983) (“A grudging or negative attitude by reviewing courts toward warrants is inconsistent with the Fourth Amendment’s strong preference for searches conducted pursuant to a warrant[;] courts should not invalidate warrants by interpreting affidavits in a hypertechnical, rather than a commonsense, manner.” (brackets, quotation marks, ellipsis, and citations omitted)); ***Commonwealth v. Mendoza***, 287 A.3d 457, 462 (Pa. Super. 2022) (stating that the issuing authority must view the affidavit “in a common

sense, nontechnical, ungrudging and positive manner.” (quoting **Commonwealth v. Baker**, 615 A.2d 23, 25 (Pa. 1992)).

Pertinently, constitutional mandates “prohibit[] a warrant that is not particular enough and a warrant that is overbroad.” **Young**, 287 A.3d at 919-20 (citation omitted). We have explained that

[t]hese issues are separate but related. A warrant unconstitutional for its lack of particularity authorizes a search in terms so ambiguous as to allow the executing officers to pick and choose among an individual’s possessions to find which items to seize. This will result in the general “rummaging” banned by the Fourth Amendment. On the other hand, a warrant unconstitutional for its overbreadth authorizes in clear or specific terms the seizure of an entire set of items, or documents, many of which will prove unrelated to the crime under investigation. An overbroad warrant is unconstitutional because it authorizes a general search and seizure.

Id. at 920 (quotation marks, brackets, and citations omitted).

“[T]he natural starting place in assessing the validity of the description contained in a purportedly overbroad warrant is to determine for what items probable cause existed.” **Id.** (quoting **Commonwealth v. Green**, 265 A.3d 541, 551 (Pa. 2021)).

After establishing the scope of probable cause, the sufficiency of the description must then be measured against those items for which there was probable cause. An unreasonable discrepancy reveals that the description was not as specific as was reasonably possible. Any unreasonable discrepancy between the items for which there was probable cause and the description in the warrant requires suppression.

Id. (brackets, quotation marks, and citations omitted).

Instantly, addressing Appellant's claim that the December 2020 search warrant failed to set forth probable cause that Appellant possessed a cell phone at the time of the shooting, the suppression court opined that the ubiquity of cell phones is a "modern day reality[.]" Suppression Court Opinion, 1/2/25, at 26. The suppression court found persuasive the California Court of Appeals' following analysis on this topic:

It is [] a matter of indisputable common knowledge that most people carry cell phones virtually all the time, and courts may take judicial notice of "facts and propositions that are of such common knowledge ... that they cannot reasonably be the subject of dispute." (Evid. Code, § 452, subd. (g).) In 2018, the United States Supreme Court observed that individuals "compulsively carry cell phones with them all the time." **Carpenter v. United States**, [585 U.S. 296,]311 [(2018)] ("While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time.") Other courts have followed suit in recognizing that nearly everyone regularly carries a cell phone. **U.S. v. James** 3 F.4th 1102, 1105 (8th Cir. 2021) ("Even if nobody knew for sure whether the suspect actually possessed a cell phone, the judges were not required to check their common sense at the door and ignore the fact that most people 'compulsively carry cell phones with them all the time.'"); [**Matter of Search of Info. that is Stored at Premises Controlled by Google LLC**, 579 F.Supp.3d 62, 78 (D.D.C. 2021)] ("The core inquiry here is probability, not certainty, and it is eminently reasonable to assume that criminals, like the rest of society, possess and use cell phones to go about their daily business."). **The common knowledge that most people carry cell phones gave the issuing [authority] a substantial basis for concluding there was a fair probability that the suspects were carrying cell phones at the time of the shooting.**

Price v. Superior Court, 93 Cal. App. 5th 13, 39 (2023) (brackets in original omitted; emphasis added; punctuation and some citations modified); Suppression Court Opinion, 1/2/25, at 27.

Regarding geofence warrants and constitutional overbreadth, the suppression court further found the **Price** Court's following observation instructive:

[I]f a geofence warrant is narrowly tailored, in its initial search parameters, or geographic scope and time period, to maximize the probability it will capture only suspects and witnesses, and to minimize searches of location data and identifying information of individuals for whom there is no probable cause to believe were suspects or witnesses (uninvolved individuals), then the discretion afforded to the executing officer by Google's multistep production protocol will be constitutionally immaterial.

Price, 93 Cal. App. 5th at 41; Suppression Court Opinion, 1/2/25, at 27-28.

Accepting the pervasiveness of cell phones utilizing LH services, the suppression court rejected Appellant's arguments that the instant geofence warrants lacked particularity in establishing probable cause and were overbroad:

[T]he warrants issued in this case were both supported by probable cause and "a model of particularity" for the following reasons ...:

A. Almost immediately after being shot, Cramer called 911 dispatch while he was driving on [Route] 309 to report where he was and what had just occurred.

B. Specifically, at approximately 9:24 p.m. on January 23, 2019, Cramer called the 911 dispatch center to report that he had been shot while driving northbound on [Route] 309. Cramer provided the mile marker and exit sign information to dispatch as well as the exit off of [Route] 309 that the [maroon] vehicle had utilized while Cramer was following.

C. Trooper Tray interviewed Cramer at approximately 12:10 a.m. on January 24, 2019, in the Emergency Department at Abington Hospital. Cramer provided

information regarding where he had been just before getting on [Route] 309 and where he was going[,], when a maroon vehicle pulled directly in front of his [Tundra] after passing him on the right shoulder.

D. A witness later confirmed that at about this same time[,], he had seen [a vehicle matching the description of Cramer's Tundra] driving in the left lane northbound on [Route] 309 and witnessed as the truck merged into the right lane, forcing another vehicle onto the shoulder to the right.

E. Investigators canvassed the areas Cramer reported that he had been to prior to and after the incident, confirming [via] surveillance footage at least one of the places where Cramer had been and at what time.

F. Perhaps most importantly, **investigators were able to review the recorded 911 call Cramer made during which his locations and times [were] documented.**

G. Based upon this information, Trooper Tray applied for a geofence warrant, as required by Google, providing two very specific geographic locations during a time period of seven (7) minutes from 9:20 p.m. to 9:27 p.m. on January 23, 2019.

H. In the affidavit of probable cause, Trooper Tray explained that Route 309 and the surrounding local roads are sparsely traveled at that time of day, and therefore[,], it would be unlikely that a vast number of vehicles containing cellular devices would be located within either of the search parameters.

I. Additionally, the target location that included the Highland Avenue exit is residential, with schools, athletic fields, and single-family homes.

J. The geofences encompassed only the two areas where the suspect vehicle was believed to have been at the time of the offense and immediately thereafter, at a time when there was a significantly diminished

possibility that anyone uninvolved, either as the suspect or a witness, would be located.

The geofence warrants presented to Judge Carpenter by Trooper Tray were narrowly tailored in their initial search parameters and time period to maximize the probability that they would capture only suspects and witnesses, and minimized searches of location data for individuals for whom there was no probable cause to believe they were suspects or witnesses. The geofence warrants in the instant case were not overbroad.

....

[The suppression] court has reviewed the information offered by law enforcement in a commonsense and non-technical manner and concludes that there is substantial evidence of record as well as case law to support Judge Carpenter's decision to issue the challenged warrants. The issuing authority in this case properly determined that Trooper Tray established probable cause in his affidavits. Accordingly, [the suppression c]ourt determined that the Commonwealth demonstrated by a preponderance of the evidence that all of the challenged evidence was properly obtained.

Suppression Court Opinion, 1/2/24, at 29-32 (emphasis added).

Upon review, the suppression court's factual findings are supported by the record, and we agree with its legal conclusions. For the following reasons, we conclude that, under these particular circumstances, the geofence warrants established an individualized probability that the specific information sought would yield evidence of the shooting that occurred on Route 309, between 9:20 p.m. to 9:27 p.m. on January 23, 2019.

As the suppression court explained, the United States Supreme Court has recognized, as a matter of common knowledge, that cell phones and their services are ubiquitous and their usage universal. ***See id.*** at 27; ***see also***

Riley v. California, 573 U.S. 373, 385 (2014) (“[M]odern 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.”); **Commonwealth v. Dunkins**, 263 A.3d 247, 251 (Pa. 2021) (quoting **Carpenter**, above); **Commonwealth v. Gallagher**, 263 A.3d 1207, 1210 (Pa. Super. 2021) (*en banc*) (quoting **Riley**, above). Moreover, the December 2020 search warrant set forth that “[g]reater than 50% of all cellular devices in the United States operate on the Android system[,]” which provides the LH services law enforcement sought to query in the instant case. Exhibit C-1 at 6.

Jacoby, supra, and **Ani, supra**, cited by Appellant to support his first issue, are distinguishable. In **Jacoby**, the defendant challenged, *inter alia*, the search warrant authorizing law enforcement to search the defendant’s residence for a .32 caliber firearm approximately fifteen months after a firearm-related homicide. **Jacoby**, 170 A.3d at 652. The affidavit supporting the search warrant contained the following averments: (1) a .32 caliber shell casing was found at the scene of the murder; (2) the defendant was the registered owner of a .32 caliber firearm; (3) witnesses observed a man fitting the defendant’s description at the scene of the crime on the date of the murder; (4) a witness observed a vehicle matching the description of a van used by the defendant at the crime scene on the date of the murder; and (5) because the defendant was a person prohibited from possessing firearms, “it

is reasonable to believe [the defendant] would retain [his .32 caliber firearm], as he is barred from legally obtaining another hand-gun.” **Id.** at 653-54.

The **Jacoby** Court rejected the defendant’s argument that the affidavit failed to set forth probable cause that the defendant was present at the scene of the crime and that he owned a .32 caliber firearm. **Id.** at 654. The Court found merit, however, in the defendant’s claim that the warrant application lacked individualized suspicion leading to a probability that the firearm sought would be found in the defendant’s home fifteen months after the murder. **Id.** The Court concluded that

[p]robable cause to search [the defendant’s] home did not exist simply because probable cause existed to believe that he had committed the murder, with a weapon of the same caliber as one that he owned, and then drove in the general direction of his home fifteen months before the search warrant was issued. Together and by themselves, these factors do not justify entry without some nexus to the home.

Id. at 656.

In **Ani**, which involved a series of college campus burglaries, the warrants in question sought, *inter alia*, the following from the defendant’s cell phone: (1) photographs or recordings of stolen items; (2) communications concerning the crimes; (3) geolocation data at the time of the burglaries; and (4) data related to the cell phone’s flashlight application. **Ani**, 293 A.3d at 709-11.

The **Ani** Court concluded that **Jacoby**

hold[s] that categorical assumptions cannot be the sole justification for probable cause. In that respect, the affidavit here

is even weaker than the flawed affidavit in **Jacoby**, because these affidavits did not even attempt to claim that home invaders are likely to have used their phones to aid the commission of their crimes. ... As reflected in the very first warrant application—the suppression of which the Commonwealth does not challenge—the affiants merely speculated that the phone may contain evidence of the crime.

Id. at 727 (citation omitted); **see also id.** at 728 (“[T]he notion that [the defendant] took evidence of his ‘trophy’ or videotaped his crimes rested on pure conjecture.”).

While the **Ani** Court determined that the majority of the items sought in the Commonwealth’s warrant applications were not supported by probable cause, it concluded that the warrant seeking “locational data and any evidence concerning flashlight usage” were supported by individualized suspicion: “[The warrant] specifically delineated several items, and ... was quite limited in temporal scope, as it was confined to the three known incident dates. ... **[T]hose temporal restrictions are relevant and[,]** **as drawn[,]** **the warrant did contain a check on the officers’ authority.**” **Id.** at 730 (emphasis added).

Thus, in **Jacoby** and **Ani**, law enforcement ran afoul of the defendants’ rights against unreasonable searches by failing to articulate any specific nexus between the evidence to be obtained and the items searched. In **Jacoby**, law enforcement assumed that the defendant, a person prohibited from firearms possession, would have kept his gun in his home fifteen months after the homicide. In **Ani**, law enforcement speculated that the defendant may have

taken photographs or videos of stolen items. Accepting these types of general assumptions would enable law enforcement to justify virtually any search.

We find our decision in **Kurtz, supra**, a more apt comparison. In **Kurtz**, police linked the defendant to a sexual assault on the victim (K.M.), after police had obtained a search warrant for records of Google search engine results related to K.M.'s name and home address. **Kurtz**, 294 A.3d at 517. The search warrant requested search engine records pertinent to the investigation from the week preceding the sexual assault. **Id.** Google provided police with an internet protocol (IP) address from which two relevant searches were conducted, leading to the discovery and arrest of the defendant. **Id.** The trial court thereafter denied Appellant's motion to suppress, *inter alia*, the incriminating search engine results connected to Appellant's IP address. **Id.** at 518.

On appeal, the defendant challenged the search warrant as "merely speculative" and as not setting forth "grounds that an individual of reasonable caution would believe that the perpetrator of the assault of K.M. used the Google search engine when planning the crimes." **Id.** at 519. In rejecting Appellant's argument, we agreed with the trial court that the search warrant showed a "fair probability" that the information sought would "uncover evidence related to K.M.'s sexual assault," and emphasized the "practical, common sense assessment" the circumstances set forth in a search warrant affidavit must be afforded. **Id.** at 524. We explained,

[i]t was reasonable to conclude, **due to the ubiquity of internet search engines and Google's services in particular**, that the planning of the crime would take advantage of Google's search engine.

Moreover, we are unpersuaded by Appellant's claims that the affidavit was improperly based upon "general assumptions rather than specific and articulable facts" and that it lacked "concrete evidence" that the perpetrator of K.M.'s assault used Google. The search warrant did not simply assert that a crime occurred at a certain place and ask for all Google searches related to that location. Instead, [the affiant] articulated various circumstances he discovered during his investigation indicating that the crime was well-planned, including the secluded locations of K.M.'s house and the field where K.M. was dropped off, the timing of the crime when K.M.'s husband was at work, and the typical profile of perpetrators of this type of sexual assaults. Furthermore, **Appellant's contention that the warrant needed to lay out "concrete evidence" that Appellant had used Google's services, is in conflict with the probable cause standard, which requires only that there is a "fair probability" that the search will be fruitful. *Commonwealth v. Harlan*, 208 A.3d [497,] 505 [(Pa. Super. 2019)]** (citation omitted). Granting the appropriate deference to the issuing authority's probable cause determination, we see no error in the trial court's conclusion that the facts alleged in the warrant were sufficient to warrant an individual of reasonable caution to believe that a search should be conducted. ***Commonwealth v. Pacheco*, 263 A.3d [626,] 645 [(Pa. 2021)]**.

Id. (some citations and footnote omitted; emphasis added).

Here, as in ***Kurtz***, the Commonwealth was not required to set forth "concrete evidence" that Appellant was using a cell phone with Android-based location services. Instead, the Commonwealth appropriately relied on the "fair probability" standard, borne out by the ubiquity of cell phone usage, that a

majority of cell phone users utilize Android-based services,¹⁹ and that Appellant likely possessed such a device. Because pervasive cell phone possession and cell phone service usage is a matter of common knowledge, and because law enforcement combined this common knowledge with specific factual circumstances regarding the time and place of the crime, we reject Appellant's argument that the December 2020 search warrant relied upon "categorical assumptions."

We further conclude Appellant's claims of overbreadth and lack of particularity likewise fail. As noted above, Pennsylvania (and much of the country), has not had occasion to consider the lawfulness of the geofence procedure, whereby law enforcement seeks LH data to narrow the pool of suspects of a known crime. Nevertheless, we determine the geofence procedure employed in the instant case comports with the foundational principles (described above) setting forth the parameters of constitutionally sound search warrant applications.

We find persuasive the rationale set forth in ***Jones v. State***, 913 S.E.2 700 (Ga. 2025), involving a geofence procedure identical to the one employed in the instant case. In ***Jones***, the defendant

was charged with murder after the police identified her using the [LH data] from her cell phone. The police got that [LH data] through search warrants that authorized the police to obtain from Google an anonymized list of devices that reported their locations

¹⁹ We note that Appellant does not challenge the veracity of the facts set forth in the December 2020 search warrant.

within 100 meters of the victim's home during the four hours when the murder happened — a process known as "geofencing" — and identifying information tied to the subset of devices that were relevant to the investigation. Before trial, Jones moved to suppress the evidence from the geofence warrants, arguing that the warrants violated the Fourth Amendment to the United States Constitution because they were not supported by probable cause and failed to satisfy that Amendment's particularity requirement. The trial court denied the motion, and [the Georgia Supreme Court] granted Jones's application for an interlocutory appeal.

Id. at 703.

Affirming the trial court, the ***Jones*** Court noted that the

warrant applications explained[,] among other things[,] that the suspect was caught on video using a cell phone near the victim's home, that many cell phones generate Google [LH] data, and, later, that the movements of a specific cell phone "matched up" with what was known of the suspect's movements. That information, together with the reasonable inferences and common sense that a reviewing magistrate may draw on in assessing probable cause, gave the magistrate here a substantial basis for concluding that accessing the [LH data] and identifying information sought from Google had a fair probability of helping the police identify the unknown murder suspect in the video. And the warrants satisfied the particularity requirement because they gave the police specific guidance as to what information they were authorized to access — a list of anonymized Google IDs and location history data from devices reporting their locations within 100 meters of the victim's home during a given time frame, and then identifying information tied to one of those Google IDs — and avoided the kind of unfettered discretion that would pose a particularity problem.

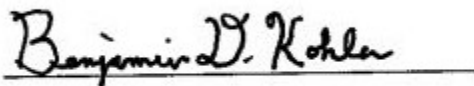
Id. at 703-04.

Instantly, the December 2020 search warrant requested that Google query an anonymized list of LH data related to device IDs within two specific geographic locations along Route 309, within a seven-minute time frame. Like the ***Jones*** Court, we conclude that Google's prophylactic measure of

anonymizing device IDs, prior to providing them to law enforcement, “avoided the kind of unfettered discretion that would pose a particularity problem.” ***Id.*** at 704. Moreover, as the warrant “described as particularly as reasonably possible the items for which there was probable cause[,]” we conclude that it was not overbroad. ***Green***, 265 A.3d at 553 (citation omitted). Given the narrowly-tailored geographical and temporal range of the information sought in the warrant application, the warrant set forth “a fair probability that contraband or evidence of a crime” would be found within the anonymized list law enforcement sought. ***See Kimmel***, 331 A.3d at 30. Accordingly, Appellant’s issues merit no relief.

Judgment of sentence affirmed.

Judgment Entered.

A handwritten signature in black ink, reading "Benjamin D. Kohler", is written over a horizontal line.

Benjamin D. Kohler, Esq.
Prothonotary

Date: 9/18/2025