

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

In the Matter of the Application for Tower
Dump Data for a Sex Trafficking Investigation

23 M 87

Magistrate Judge Sunil R. Harjani

MEMORANDUM OPINION AND ORDER

Before the Court is a warrant application for cell tower data, also known as a tower dump warrant. More specifically, the government seeks to obtain cell phone numbers and identifiers for cell phones that connected to cell towers at five locations at a particular time to determine the identity of suspects involved in multiple acts of sex trafficking and assault. This warrant request, by its very nature and name (a “tower *dump*”), sweeps broadly and may collect information on individuals who participated in the crime, but will undoubtedly collect information on individuals who are not involved whatsoever in the underlying criminal activity. The Court has previously addressed similar issues with respect to other canvassing warrants, such as for Google geofence data and cell-site simulator data. *See In the Matter of the Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F.Supp.3d 345 (N.D. Ill. 2020); *In the Matter of Use of a Cell-Site Simulator to Identify a Cellular Device in a Narcotics Trafficking Case*, 2022 WL 3645982 (N.D. Ill. Aug. 24, 2022). In these opinions, the Court has requested and approved various protocols or limitations as a condition of allowing the government to obtain location data in order to ensure that the warrant satisfies Fourth Amendment principles of probable cause and particularity, and addresses overbreadth concerns in light of the inherently broad nature of the warrant request. The government’s initial submission to this Court seeking a

tower dump warrant did not have any protocols. At this Court's request, the government resubmitted the warrant application with certain protocols to address the Court's concern discussed herein. As further explained below, the Court has authorized the warrant in this case with these protocols, as follows: (1) the government may seize data only when there is overlap between two or more locations; (2) the government has represented that it will not use further investigative steps concerning data that does not meet the above requirement; and (3) the government will secure the remaining data with a law enforcement agent or employee that is not involved in the investigation. With these limitations, the Court finds that the proposed warrant satisfies Fourth Amendment concerns, and the Court has signed the warrant. The Court issues this opinion to explain its rationale for authorizing the warrant, and given the dearth of opinions that address this matter.¹

BACKGROUND

On January 31, 2023, the government submitted an application and affidavit in support of a proposed warrant ("Aff.") for this Court's consideration in a multiple incident, multiple suspect sex trafficking investigation. The affidavit details five armed attacks on six victims in the Chicagoland area. Aff. ¶¶ 6-12, 33-36, 42-48, 58-66, 78-82. The affidavit further provides probable cause that all five attacks were likely orchestrated by the same individuals and involved incidents of sex trafficking. *Id.* ¶¶ 6, 39-41, 73-75, 88. Moreover, there is evidence that the suspects were in possession of cell phones during some of the attacks.² *Id.* ¶¶ 6, 11 18, 37, 58, 63, 69-70, 85.

¹ The government has opted to seek a search warrant under Federal Rule of Criminal Procedure 41. Thus, the Court applies established Fourth Amendment principles in evaluating the warrant, and does not address whether a warrant is required for tower dump data, an issue the Supreme Court left open in *Carpenter v. United States*, 138 S.Ct. 2206, 2220 (2018).

² Because the warrant and its supporting materials remain under seal, the Court does not provide a fulsome description of the facts of the alleged criminal activity in this opinion.

With this warrant request, the government seeks historical cell phone records for all cell phones that connected to cell towers in the five locations where the alleged attacks occurred. Aff. ¶¶ 94-96. In general, cellular telephone companies maintain antenna towers or cell towers that provide cellular service to devices that are within range of the tower's signal. *Id.* ¶ 90. By communicating with a cell tower, a cell phone can transmit and receive communications, such as phone calls, text messages, and other data. *Id.* Cellular phone companies maintain records that allow them to determine which wireless device used cellular towers on the provider's network to send and receive messages. These records may include the telephone number and unique identifiers of the device, such as an Electronic Serial Number (ESN), a Mobile Electronic Identity Number (MEIN), a Mobile Identification Number (MIN), a Subscriber Identity Module (SIM), a Mobile Subscriber Integrated Services Digital Network Number (MSISDN), an International Mobile Subscriber Identifier (IMSI), or an International Mobile Equipment Identity (IMEI). *Id.* ¶ 91. Other records may include the sector of the tower where the connection was made, the time, date, and duration of the communication, and the telephone numbers associated with any communication. *Id.* ¶ 92. Thus, by obtaining phone numbers connecting to cell towers near where a crime occurred, the government can potentially identify suspects of the crime by tracing the phone number back to individuals. The government seeks cell tower data for any cell phone connecting to a tower at these five locations for a period of time ranging between thirty minutes and one hour. *Id.* ¶¶ 94-96. According to the government, "by cross referencing the information to identify cellular devices that were active and present in two or more of these areas and/or communicated with one another, the information can be used by law enforcement to identify potential suspects." *Id.* ¶ 94. That is, given that the same individuals likely committed the offense, a cell phone number that appears connected to cell towers in two or more locations would make it

more likely that the number belonged to the perpetrator of the crime.

DISCUSSION

A warrant that authorizes a cell tower dump is, by its very nature, allowing the government to obtain cell phone numbers of individuals who may be involved in the offense, but most definitely third parties not involved in the offense. Indeed, that is the very purpose of a tower dump request—to obtain cell numbers of everyone in the vicinity of the crime, and through cross-referencing and the process of elimination, narrow the pool of phone numbers that could belong to the suspect of the crime. Once that pool has been determined, the government can use other investigative tools, such as a grand jury subpoena which does not require court authorization, to obtain subscriber information for that cell phone, and thus have the identity of a potential suspect of the crime.

However, armed with cell phone identifiers and without any imposed limitations, the government could discover the identity of any those individuals, irrespective of their involvement in the crime, and their location information. How many uninvolved individuals' cell numbers will be collected through a tower dump is unknown, but in a dense urban city, it is fair to say that the numbers could be in the hundreds, thousands, or hundreds of thousands. This location information, now in the possession of the government, could include not only public places (roads and bridges), but more importantly non-public places, such as homes, businesses, churches, mosques, hospitals, and political offices. This implicates privacy concerns of those uninvolved in any criminal activity, who are merely going about their daily lives and presumably do not want their movements tracked by the government, particularly in private and sensitive spaces. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (cell-site data “provides an intimate window into a person’s life, revealing not only his particular movements, but through them his familial, political,

professional, religious, and sexual associations.”) (internal quotations omitted). Awareness that the government may be watching chills both expression and association. *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *see also People v. Weaver*, 909 N.E.2d 1195, 1199 (N.Y. 2009) (“Disclosed in the [GPS] data ... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.”) And, without restrictions, “with just the click of a button, the Government can access each carrier’s deep repository of historical location information at practically no expense.” *Carpenter*, 138 S. Ct. at 2218.³

At the outset, and to be clear, the question of whether there is probable cause to authorize the collection of cell tower dump data is not a difficult one. In examining an application for a warrant, the Court must inquire as to whether probable cause exists that a crime has been committed and that evidence of the crime will be located at the place to be searched. *Illinois v. Gates*, 462 U.S. 213, 238 (1983); *United States v. Hall*, 142 F.3d 988, 995 (7th Cir. 1998). Put simply, probable cause is a fair probability that contraband or evidence of a crime will be found in a particular place, based on the totality of the circumstances. *Gates*, 462 U.S. at 238. Probable cause does not require conclusive evidence that links a particular item to a crime. *United States v. Anderson*, 450 F.3d 294, 303 (7th Cir. 2006) (citation omitted). “Rather, issuing judges may draw reasonable inferences about where evidence is likely to be found based on the nature of the evidence and the offense.” *United States v. Zamudio*, 909 F.3d 172, 175 (7th Cir. 2018).

³ The government also cannot credibly argue that no privacy interests are at stake here, as the government is the one that is asking this Court for a warrant under the Fourth Amendment, thus recognizing for present purposes that there is a reasonable expectation of privacy in one’s location data in connection with a tower dump warrant.

The agent's affidavit easily establishes probable cause that a crime has been committed. Through surveillance footage and victim interviews, the affidavit establishes probable cause that victims were assaulted in the course of sex trafficking at five locations in the Chicagoland area. The affidavit also establishes probable cause that evidence of the crime will be located at the cellular telephone service providers. The suspects of the crime were seen either holding cell phones and/or making telephone calls on surveillance footage, and thus those phones were likely connected to cell towers at the time of the alleged crime. *Aff.* ¶¶ 6, 11 18, 37, 58, 63, 69-70, 85. As a result, there is a fair probability that the cell phone carriers will have records that reveal the cell phone numbers of the perpetrators of the alleged crime. *See United States v. James*, 3 F.4th 1102, 1105 (8th Cir. 2021) (holding that, in a crime involving multiple robberies by a single individual, there was sufficient probable cause for a tower dump warrant in order to identify a common number present at the locations of the robberies); *see also United States v. Vizcarra-Millan*, 15 F.4th 473, 505 (7th Cir. 2021) (explaining the warrant application was strong given the central role of cell phones to the gang).

The more pertinent issue is particularity and overbreadth. The Fourth Amendment requires that warrants “particularly describ[e] the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “The manifest purpose of this particularity requirement was to prevent general searches.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). The particularity requirement “ensures 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.” *Id.*; *see also Marron v. United States*, 275 U.S. 192, 196 (1927) (“The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another.”). The particularity

requirement also “ensures that the scope of a search will be confined to evidence relating to a specific crime that is supported by probable cause.” *United States v. Vitek Supply Corp.*, 144 F.3d 476, 481 (7th Cir. 1998).

In contrast, “[w]arrants that are overbroad, that is, that allow officers to search for items that are unlikely to yield evidence of the crime, violate the Fourth Amendment.” *United States v. Vizcarra-Millan*, 15 F.4th 473, 502 (7th Cir. 2021). A warrant with an “indiscriminate sweep” is “constitutionally intolerable.” *Stanford v. Tex.*, 379 U.S. 476, 486 (1965). As the proper scope of a warrant is confined to the breadth of the probable cause that supports it, “the requirement of particularity is closely tied to the requirement of probable cause.” *United States v. Griffith*, 867 F.3d 1265, 1275 (D.C. Cir. 2017). “[A] broader sweep,” however, may be permissible “when a reasonable investigation cannot produce a more particular description” prior to obtaining and executing the warrant. *Id.* at 1276 (citing *Andresen v. Maryland*, 427 U.S. 463, 480 n.10 (1976)).

The warrant in this matter has three specific characteristics that serve to address issues of particularity and overbreadth. First, the warrant is constrained in both geographical and temporal scope. The warrant requests cell tower data only for the cell towers near the location of the crimes. The warrant provides the addresses or street intersections where the crime took place. Aff. ¶¶ 7, 23, 42, 51, 78. The warrant also has the specific time range, which varies between thirty minutes and one-hour intervals, at these five locations depending on the duration of the crime based on surveillance footage and victim interviews. *Id.* ¶ 95. The warrant also authorizes a seizure of data only when a phone number hits two or more towers, increasing the probability significantly that the data seized will yield a fair probability that it belongs to the suspect of the crime. *Id.* ¶ 97.

Second, the warrant states that “[l]aw enforcement will not take further investigative steps with regards to identifiers collected from the Providers, including issuing grand jury subpoenas

relating to those identifiers, except for identifiers related to devices that utilized cellular towers at more than one of the locations and time pairs[.]” Aff. ¶ 97. This provision ensures that the government is not given the authority to obtain subscriber information, and thus determine the location of all individuals at its whim, but rather when there is a fair probability that the individual could be a suspect. A fair probability, in this context, is when an individual is present in two or more locations of a crime scene.

Third, the warrant states that after seizure of the items that meet the above requirements, “the original records provided by the Provider are to be retained by a law enforcement agent or employee who is not involved in the investigation and will not be accessed by the investigative team until further order of the court.” Aff. ¶ 98. Once again, by removing the irrelevant information from the hands of the investigative team, this restriction further protects third-party privacy interests.

It is worth noting that with protocols two and three, there are real tangible benefits with these limitations. Without the use of a subpoena (or other investigative means) to identify the subscriber, the government is merely left with cell phone identifiers. Cell phone numbers and identifiers without a name have a lesser impact on an individual’s privacy because the numbers alone do not identify the name of the person using the phone, and thus do not directly reveal an individual’s location at a particular place and time. Cell tower dump data also has a lesser privacy interests than, say GPS data, because it does not pinpoint the location of a person, but rather informs law enforcement as to what tower or sector of that tower a phone made a connection. But while it may be lesser, the privacy interest is not zero. Like a social security number or a driver’s license number, it takes only a minor step by law enforcement to connect an individual to that number, which opens up a treasure trove of data. Indeed, with cell phone numbers, a publicly

available reverse phone lookup website is often all that is necessary to determine identity. Therefore, once potential suspects' numbers are identified and subscriber information obtained, the protocols restricting further use of the remaining phone numbers and the segregation of that data can prevent any further invasion of third-party privacy interests.

The Court also recognizes that these protocols are not bullet-proof. That is, none of these limitations will prevent a situation where an innocent person's cell tower data overlaps. For example, a phone number of a person living in a residence between two towers will most certainly appear at both towers, and thus satisfy the "multiple locations" criteria. But the Fourth Amendment does not require law enforcement to use a scalpel in its investigations. The inherent nature of authorizing a search warrant is to permit law enforcement to conduct a *search for evidence* in places where there is only a *probability*, not a certainty, that evidence will be found. *See, e.g., James*, 3 F.4th at 1105 (rejecting the argument that a cell tower dump warrant required absolute certainty that the robber possessed a cell phone); *United States v. Aljabari*, 626 F.3d 940, 944 (7th Cir. 2010) ("often, nothing will *directly* indicate that evidence of a crime will be found in a particular place. For that reason, an affidavit need only contain facts that, given the nature of the evidence sought and the crime alleged, allow for a reasonable inference that there is a fair probability that evidence will be found in a particular place") (emphasis in original). But in some places where a search is being conducted, there is remarkably often a *certainty* that law enforcement will view personal information that has nothing to do with the crime along with the incriminating evidence. Belongings of house guests present during searches of a suspect's residence, or intimate and personal emails from a third-party sent to a suspect are but two examples of where a law enforcement search will impact a third-party's privacy interest. *See also Dahlia v. United States*, 441 U.S. 238, 257-58 (1979) ("Often in executing a warrant the police may find it

necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant”). Indeed, the starkest example of this concept is found in the Supreme Court’s decision in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1970). There, the Supreme Court permitted a search of an office pursuant to a warrant to stand when there was *no* evidence that the occupants of the office had any involvement in criminal activity. *Id.* Rather, the warrant application only demonstrated probable cause that evidence of the crime would be located in that office. The Supreme Court further noted, “[n]othing on the face of the [Fourth] Amendment suggests that a third-party search warrant should not normally issue.” *Id.* at 554.

As this Court has stated, in any search scenario, law enforcement will implicate privacy concerns of uninvolved individuals. But merely because uninvolved individual’s privacy interest are impacted does not mean that a court cannot authorize those searches. *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 84 (D.D.C. 2021) (“The Fourth Amendment was not enacted to squelch reasonable investigative techniques because of the likelihood—or even certainty—that the privacy interests of third parties uninvolved in criminal activity would be implicated.”). Put another way, there is a difference between searching and rummaging under the Fourth Amendment. *United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010) (“The Fourth Amendment requires that a warrant describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging through one’s belongings.”). Rummaging has no boundaries and no limitations. So while law enforcement need not use a scalpel, they are prohibited from using a sledgehammer. The balance in the Fourth Amendment—between individual privacy and law enforcement interest—is somewhere in between. *Maryland v. King*, 569 U.S. 435, 448 (2013) (courts weigh “the promotion of legitimate governmental interests” against “the degree to which [the search] intrudes upon an individual’s privacy.”) (quoting

Wyoming v. Houghton, 526 U.S. 295, 300 (1999)). In this case, the cell tower dump warrant is supported by evidence sufficient to satisfy the probable cause standard, particularly describes the place to be searched and the items to be seized, is sufficiently cabined in terms of geography, time, and the requirement of overlapping tower data, and has the means and methods to deal with uninvolved third-party data that cannot be avoided in the receipt of tower dump data. That is a tower dump warrant that complies with the Fourth Amendment, as it maintains that balance and is reasonable under the circumstances. *Id.* (“we must evaluate the search or seizure under traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.”).

The Seventh Circuit has not yet considered the broad nature of a tower dump and the consequences of authorizing a warrant of this scope. In *United States v. Atkinson*, 916 F.3d 605 (7th Cir. 2019), the Seventh Circuit primarily found that there was no Fourth Amendment violation because T-Mobile voluntarily turned over tower dump information, without a warrant, in order to protect its own interests to avoid more robberies of its store. Because no warrant was involved, the Court did not address the scope of any warrant request associated with tower dumps. But this Court is not alone in expressing its concern, and requiring protocols, with respect to tower dump warrants. Other judges have required variations of the above protocols to ensure compliance with Fourth Amendment principles. For example, *In the Matter of Search of Information Associated with Cellular Telephone Towers*, 2022 WL 2922193 (D.D.C. Jul. 25, 2022), the court found that the tower dump warrant satisfied overbreadth concerns because: (1) it had a narrow geographical and temporal scope, and (2) the government represented that data that was not relevant to the investigation would be segregated without further review, absent a court order. As another

example, *In re Search of Cellular Tel. Towers*, 945 F.Supp.2d 769 (S.D. Tx. 2013), in order to address concerns about uninvolved individual's privacy rights, the court ordered the government to return originals and copies of records to the cell service provider of information not relevant to the investigation. *See also In re Application for an Order Pursuant to 18 U.S.C 2703(c)*, 42 F.Supp.3d 511, 519 (S.D.N.Y. May 30, 2014) (holding, pre-*Carpenter*, that a warrant was required for tower dump data and ordering the government to "outline[] a protocol to address how the Government will handle the private information of innocent third-parties whose data is retrieved."). Further, in *Commonwealth v. Perry*, 489 Mass. 436 (2022), the Massachusetts Supreme Court held not only that a search warrant was required to obtain tower dump data, but that the issuing "judge must ensure that it provides a protocol for the disposal of any data that falls outside the scope of the search" in order to protect third-party privacy rights.

Difficulties in reigning in warrants because of the inherently sweeping nature of the relevant technology are not new. In the past, courts have struggled with how to permit a search of email records from an electronic account provider, such as Google or Yahoo!. The balance that was reached, ultimately codified in a two-step process in Federal Rule of Criminal Procedure 41(e)(2)(B), is to allow the government to obtain a full copy of an electronic account from the service provider pursuant to a warrant, which may have relevant information but most definitely is chock full of irrelevant material. But, the rule provides that the government may later review that copy of the full account for specific items considered to be evidence of the criminal conduct. Fed. R. Crim. P. 41(e)(2)(B); *see also* Fed. R. Crim. P. 41 advisory committee's note to 2009 amendment ("Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location."). And once the authorized

seizure has taken place and the search completed, the government is not permitted to re-search the original, voluminous batch of electronic mail without further court authorization. That process is now also memorialized in an electronic search protocol regularly used and attached to every electronic account search warrant issued in the Northern District of Illinois.

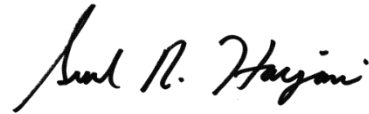
There are certainly different ways of addressing the concern associated with the potentially massive quantities of data obtained through a cell tower dump, as reflected in the above cases. In another context, the Court has required the government to delete cell-site simulator data of uninvolved individuals once the suspect phone has been identified, which is a protocol also recommended and approved by Department of Justice policy on cell-site simulators. *See* 2022 WL 3645982 at *5. While warrants cannot be open-ended searches of anyone within the vicinity of the crime without limitations, the particularity requirements cannot be so narrow they handcuff law enforcement's ability to execute the warrant. *See Aljabari*, 26 F.3d at 947 (“[An executing officer must interpret a warrant’s terms reasonably, but the officer need not give them the narrowest possible reasonable interpretation”). Particularity also turns on what is realistic or possible for the investigation at hand, *see Archer v. Chisholm*, 870 F.3d 603, 616 (7th Cir. 2017), and the protocols here are realistic in that they do not impose precision-like requirements on a technology that inherently sweeps broadly.

The Court also acknowledges that the warrant review process does not begin and end with the magistrate judge's authorization of the search. Warrants are later subject to review for reasonableness, particularly by district judges when considering motions to suppress. *Dalia*, 441 U.S. at 258 (“the manner in which a warrant is executed is subject to later judicial review as to its reasonableness”). As such, at the back end, the Fourth Amendment constrains government action – the caveat of course is that the good faith exception tends to save most searches conducted

pursuant to a warrant. *See United States v. Leon*, 468 U.S. 897 (1984). And innocent third parties have no means of learning that their cell phone data was disclosed to the government, which makes any kind of future legal action on their part nearly impossible. Which is why, once again, the initial review of the warrant for reasonableness by a neutral and detached magistrate judge is so critical.

The government's proposed protocols here, at this Court's request and in the tower dump context, is merely one method of safeguarding third-party privacy interests. Other protocols may also suffice. But in this Court's view, the present warrant with its limitations satisfies the stated concerns. Accordingly, the Court has authorized the collection of tower dump data and issued the warrant.

SO ORDERED.



Dated: February 6, 2023

Sunil R. Harjani
United States Magistrate Judge