STATE OF NORTH CAROLINA IN THE GENERAL COURT OF JUSTICE

LEE COUNTY SUPERIOR COURT DIVISION

STATE OF NORTH CAROLINA ) FILE NOs. 14CRS 53533A

) 15CRS 00061A

v. ) 17CRS 00206A

)

EMMANUEL SANDERS )

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**MOTION TO SUPPRESS TOWER DUMP RECORDS**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

NOW COMES Emmanuel Sanders, *pro se,* and moves this Court pursuant to the Fourth Amendment of the United States Constitution; Article I, § 20 of the North Carolina State Constitution; the Stored Communications Act (“SCA”); and North Carolina General Statute § 15A-974, to suppress historical cell phone records from nine cell towers in Sanford, North Carolina, obtained by court order under 18 U.S.C. § 2703(d).

The use of a 2703(d) order to obtain data from nine cell towers over the course of an hour, nine so-called “tower dumps,” is not authorized by statute under the SCA. Instead, tower dumps amount to prohibited “general warrants” under the Fourth Amendment and Article I, § 20 of the North Carolina Constitution. Compelling service providers to comply with tower dump requests can implicate the privacy of hundreds or thousands of innocent people, for whom there is no probable cause to suspect of criminality. A tower dump could be used to easily identify the people at home in a neighborhood on a particular night, the protesters at a political rally, or the congregants attending a mosque, synagogue, or church. Such indiscriminate, bulk surveillance is the “chief evil” that gave rise to the Fourth Amendment and its prohibition on general warrants. *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980)).

Even if this Court does not read the SCA, the Fourth Amendment, and Art. I, § 20, to prohibit government from seeking tower dump authorizations in all circumstances, it should conclude that tower dumps require the judicial oversight provided by a probable cause warrant under *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018). In *Carpenter*, the Supreme Court held that individuals have a reasonable expectation of privacy in their physical movements as captured by cell-site location information (“CSLI”). *Id.* at 2217. Although the Court did not rule on the constitutionality of tower dumps, *id.* At 2220 (“We do not express a view on matters not before us: real-time CSLI or ‘tower dumps’”), the cell phone records at issue here share the same qualities and implicate the same constitutional concerns that animated a majority of the Court in *Carpenter*.

Tower dump records are at least as “detailed, encyclopedic, and effortlessly compiled” as CSLI, *see id.* at 2216, with the same propensity to reveal private “familial, political, professional, religious, and sexual associations.” *Id.* at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (opinion of Sotomayor, J.)). Thus, at a minimum, the government should have obtained warrant based on probable cause that the tower dumps would turn up evidence of a crime. It failed to do so. As a result, this Court should suppress all tower dump records obtained without a warrant, and all of the fruits thereof. N.C. Gen. Stat. § 15A-974. In support of this motion, the defendant shows unto the Court as follows:

**Relevant Facts**

On November 22, 2013, at approximately 5:30 in the morning, a “6’ tall black male, in his 20-30’s with shoulder length long braids (pulled back), who was around 225 lbs”[[1]](#footnote-1) broke into a trailer located on 69 Hickory Nut Ct. The man shouted, “Sheriff’s Department, get on the ground.” He was wearing a sweatshirt that said, “Sheriff’s Department” and holding a rifle. The man ordered Marjorie and Andy Giles to get on the ground. Mr. Giles moved toward the man. The man shot Mr. Giles. The man asked where “the money” was, and Mrs. Giles showed him the money. The man then ordered Mrs. Giles to lay down and he zip tied her feet together. Mr. Giles died from his injuries.

Mrs. Giles called 911 on her daughter’s cell phone at 5:48am. Officers from the Lee County Sheriff’s Office (LCSO) responded to the scene. They took the statements of Mrs. Giles and her two teenaged children, who had also been present.

Mrs. Giles reported that the man in the house had spoken to someone on a cell phone while he was there. As a result of this information, Detective Ellerby got a court order on 22 November 2013, compelling “any and all electronic communications providers” to provide “any and all transactional records pertaining to cellular telephone calls, SMS texts, evolution data optimized (EVDO) information, per call measurement data (PCMD) and direct connect information, received by or transmitted from cellular towers… that may provide service to the area in and around 69 Hickory Nut Court, Sanford, N.C.” These types of records are commonly referred to as “tower dumps.”

The stated time frame for the requested records was 5:00pm to 6:00am on 22 November 2013. Detective Ellerby initially sent a cell provider a letter explaining he had intended for the order to read 5:00am to 6:00am, but later, on 5 December 2013, he got a second order with identical language. The only difference was the corrected timeframe.

It is unclear from the provided records which order each cell service provider was responding to, but five different cell providers responded: AT&T, Sprint, T-Mobile, U.S. Cellular, and Verizon. Verizon and Sprint each provided records for three separate towers, for a total of nine dumped towers near the crime scene. U.S. Cellular provided records for the entire 24-hour period on 22 November 2013, for a total of 5,764 entries on the spreadsheet. Only 22 entries related to the intended timeframe.

In these various tower dump records, police found evidence that a phone number associated with Phillip Fortune and different number associated with Franklin Dorsett “pinged” off towers near the crime scene. Around the same time, a witness named LaQuisha Shaw was providing information that Fortune, Dorsett, Travis McLean, Wilbur Bruton, Jessica McCoy, and Akil McAdin were involved in the robbery. These six individuals were arrested and charged in this case.

In November of 2014, Brittany Chiavaro spoke to police. She said that her boyfriend, Harley Chavis, had told her he was involved in the robbery. She claimed Chavis had confessed to her and said that Derek Strickland, CJ Mintz, and “Genesis” were also involved. She claimed the robbery was planned at the house of a man named Johnathan Oakley. Johnathan Oakley was, at one time, the neighbor of Emmanuel Sanders. Police developed a theory that “Genesis” was Emmanuel Sanders.

Phone numbers associated with Strickland and Chavis were located within the tower dump records previously obtained. There were also several calls to 919-XXX-XXXX, in those tower dump records. This number was registered to Johnathan Oakley.

Chavis, Mintz, Strickland, and Mr. Sanders were all arrested and charged with these crimes. The original six co-defendants’ charges were dismissed approximately two months later.

On 21 August 2018, Johnathan Oakley met with Investigator Holly and ADAs Mike Beam and Chris Autry. At that time, he “added” to his previous statement that 919- XXX-XXXX was a phone number that belonged to Mr. Sanders and that Mr. Sanders asked him to add it to his phone plan. This information was provided in discovery to the defendant on 29 August 2018. There is no other information contained in discovery in which this phone number is described as belonging or being associated with Mr. Sanders.

**Additional Background**

Cell phone use has become ubiquitous: The number of wireless accounts now exceeds the total population of the United States;[[2]](#footnote-2) at least 95% of all American adults own cell phones; and most carry their phone with them everywhere they go.[[3]](#footnote-3) Indeed, as the Supreme Court explained in *Riley v. California*, cell phones have become “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. 134 S. Ct. 2473, 2484 (2014).

Cell phone send and receive radio signals via base stations, known as cell towers. Towers typically have multiple cell “sites” facing in three or four different directions, each containing antennae that detect and connect cell phones to the cellular network.[[4]](#footnote-4) Cell phones automatically try to connect to the nearest or strongest base station and, as users move father away from one base station and closer to another, their phone automatically transfer the connection to a new base station.[[5]](#footnote-5)

As cell phone use has increased, service providers have installed more cell sites to handle the demand. There are more than 300,000 cell sites in the United States,[[6]](#footnote-6) plus many more antennae constantly communicating with all phones in range.[[7]](#footnote-7) Traditional cell phones communicate with the wireless network through cell sites when using the phone or text messaging functions. But smartphones, used by 77% of Americans,[[8]](#footnote-8) communicate even more frequently. They regularly check for new emails and maintain a persistent Internet connection with the provider of the operating system, such as Google or Apple.[[9]](#footnote-9) Moreover, smartphone applications may run continually in the background, connecting to cell sites without a user interacting with the cell phone at all.[[10]](#footnote-10) As a result, smartphones transmit and receive vast amounts of data whenever the device is on, communicating with the carrier’s network as frequently as every seven seconds.[[11]](#footnote-11)

When cell phones communicate with the network, the service provider automatically logs and retains information about such communications. Thus, a request for information regarding all phones that communicated with multiple cell sites, such as the one in this case, is likely to reveal information about a very large number of phones. These “tower dumps,” can – and, in fact, consistently do –involve the collection of hundreds, thousands, or even hundreds of thousands of phone numbers.[[12]](#footnote-12) For example, when the FBI obtained tower dump records for several towers in Arizona in 2010, it received a staggering 150,000 individual users’ phone numbers in response.[[13]](#footnote-13) In a 2012 Colorado case, “at least several thousand people’s phones” were likely implicated in a series of cell tower dumps requested by local police.[[14]](#footnote-14)

**Argument**

1. **The SCA Does Not Authorize Tower Dumps**

The Stored Communications Act does not authorize tower dumps. In 1986, when Congress passed the SCA, the notion of a “tower dump” was not just foreign to lawmakers; it was antithetical to their purpose. Such sweeping, indiscriminate searches were Congress’s primary concern, not its legislative intent.

Congress passed the SCA, part of the Electronic Communications Privacy Act (“ECPA”), in response to the Supreme Court’s decision in *Smith v. Maryland*, 442 U.S. 735, 737 (1979), which found no reasonable expectation of privacy in basic telephone records held by a telephone company. The SCA prohibits government access to cell phone location data stored by a cell service provider, subject only to specific statutory exceptions. One of those exceptions permits requests for records belonging to specific, identified users. But its plain terms do not allow the kind of dragnet search at issue here.

The SCA authorizes an electronic communications service provider to divulge a record or other information pertaining to *a subscriber to or customer of such service*,” only pursuant to a warrant, court order, or consent. 18 U.S.C. §§ 2702(c)(1); 2703(c). (emphasis added). It does not say that the government may obtain the records first and identify subscribers later. Congress phrased § 2703(c) in the singular – “*a* subscriber” not ‘unidentified persons’ – and it did so for good reason.

The entire purpose of the SCA was to protect user privacy as technology advances. As a result, Congress chose to strictly limit the circumstances in which the government may obtain cell phone user data. *See* 18 U.S.C. § 2702; S. Rep. No. 99-541, at 3 (1986) (explaining intent to place a check on “technological advances in surveillance devices and techniques” that are available to “overzealous law enforcement agencies,” and noting the statute’s purpose “to protect privacy interests in personal and proprietary information”). The use of the singular article in § 2703(c) is part of Congress’s comprehensive scheme to strictly limit permissible government intrusions into the privacy of cell phone users. S*ee First Nat’l Bank in St. Louis v. Missouri*, 263 U.S. 640, 657 (1924) (noting the background principle that “‘words importing the singular number may extend and be applied to several persons or things,’” but explaining that “obviously this rule is not one to be applied except where it is necessary to carry out the evident intent of the statute”).

At very least, this Court should recognize that that the SCA does not explicitly address tower dumps. *See In re U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d)*, 930 F. Supp. 2d 698, 700 (S.D. Tex. 2012) (“That statute does not address cell tower dumps.”). Indeed, as one leading scholar of the SCA has observed, the SCA is “silent on court orders that seek records regarding hundreds or even thousands of users.” Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162, U. Pa. L. Rev. 373, 402 (2014).

Had Congress intended to authorize bulk requests for unknown customers’ data, it could have said so. It did not do so. *See United States v. Hayes*, 555 U.S. 415, 421–22 (2009) (assessing Congress’s use of the singular in a statute and explaining that, had Congress meant otherwise, “it likely would have used the plural”).[[15]](#footnote-15) It defies both the English language and legislative intent to read the SCA to permit broad requests for information about potentially thousands of unknown people. Congress plainly limited government record requests to identifiable suspects on an individual basis. It did not hand law enforcement a blank check to obtain cell phone records en masse.

1. **Tower Dumps Are General Warrants**

Tower dumps are a modern scion of general warrants, prohibited by both the Fourth Amendment and Art. I, § 20 of the North Carolina Constitution. Tower dumps seek private cell phone records, without a warrant, and without any inkling of whose privacy will be infringed. *See Carpenter*, 138 S. Ct. at 2217. They are the epitome of a fishing expedition, the same species of unlimited, open-ended searches that propelled a revolution and led to the adoption of the Fourth Amendment.

The failure to establish probable cause for single suspect must not be cause for invading the privacy of multitudes. Rather, such “exploratory rummaging” is the provenance of prohibited general warrants. *Coolidge v. New Hampshire*, 403 US 443, 467 (1971) (The problem posed by a general warrant is exploratory rummaging in a person's belongings.). It is also the central argument that the government advances in favor of permitting its practice of conducting tower dumps: ‘We don’t know.’

Such generalized, exploratory searches were the catalyst for the Fourth Amendment – memories fresh from a scandalous search for the author of a satirical pamphlet that criticized King George III. *See* Michael Price, *Rethinking Privacy: Fourth Amendment “Papers” and the Third-Party Doctrine*, 8 J. Nat’l Security L. & Pol’y 247, 256 (2016). Indeed, the open-ended searches at issue here are exactly the kind of “dragnet” searches that the Supreme Court cautioned against in *United States v. Knotts*. 460 U.S. 276, 284 (1983).

In *Knotts*, the Court signaled its unease with “dragnet type” searches using location-tracking technology, explicitly noting that “different constitutional principles may be applicable” to such searches. Indeed,the “‘wholesale surveillance’” of large numbers of people raises especially troubling Fourth Amendment concerns. *United States v. Marquez*, 605 F.3d 604, 610 (8th Cir. 2010); *accord* *United States v. Garcia*, 474 F.3d 994, 998–99 (7th Cir. 2007) (discussing concerns raised by “wholesale surveillance” and “mass surveillance” using GPS trackers).

Tower dumps involve the sort of “dragnet” surveillance that both the Framers and the Supreme Court have long feared. *See Carpenter*, 138 S. Ct. at 2215 (noting that the *Knotts* Court was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance.”); *see also* *In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113, 119 (E.D.N.Y. 2011) (Garaufis, J.) (“[T]he collection of cell-site-location records effectively enables ‘mass’ or ‘wholesale’ electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip.”).

The records in this case came from nine separate cell towers, owned by five different wireless carriers, for at least a full hour. One carrier produced 5,764 record entries over a 24-hour period, with just one relevant call alleged. Altogether, there were 6,779 record entries, only 12 of which are alleged to have any relevance to this case. The rest of the data belonged to non-suspects – admittedly innocent people. Or to put it another way, just 0.18% of the returned data produced evidence related to the investigation of this case. In short, the government had no cause (let alone probable cause) to search 99.82% of the private data it obtained. Such a miserable fishing expedition is the hallmark of an overbroad, unparticularized general warrant prohibited by the Fourth Amendment and Art. I, § 20.[[16]](#footnote-16)

By definition, tower dumps seek an untold amount of private cell phone records belonging to an untold number of individuals, who are unknown to the agents requesting the court order. The absence of any individualized probable cause makes a tower dump constitutionally overbroad under the Fourth Amendment and Art. I, § 20, the latter of which prohibits general warrants by name. These fundamental guarantees must, at minimum, “assure … preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. *Carpenter,* 138 S. Ct. at 2214. Here, that means recognizing a tower dump for the general warrant that it is.

Allowing the government to obtain tower-dump data risks sanctioning the sort of “general warrant” that the Fourth Amendment’s framers so reviled. *See Stanford v. Texas*, 379 U.S. 476, 481–82 (1965). As the Ninth Circuit observed, requests by “law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.” *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam); *accord United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). Surely, a reported gunshot in a residential neighborhood would not allow nonconsensual searches of every home in a several-block radius in hopes of identifying a suspect. Likewise, a theft on a busy street downtown would not permit frisks and bag searches of every person walking along the sidewalk. Dragnet searches are no more permissible when carried out using electronic means; a claim by the government that a criminal suspect whose email address it does not know sent a potentially incriminating email on a particular day would never authorize it to ask Google or Yahoo to produce a catalogue of every email sent from an internet protocol address on that day. Grants of “unbridled authority,” *Stanford*, 379 U.S. at 481, are unreasonable under the Fourth Amendment, no matter their form.

1. **A Tower Dump is a Search Under the Fourth Amendment**

Should this Court find that tower dumps are not outright impermissible, the Fourth Amendment would demand the kind of close judicial scrutiny associated with a warrant based on probable cause.

This is, in essence, a case of first impression. Tower dumps have been used with increasing frequency used in recent years,[[17]](#footnote-17) but there are few judicial opinions examining the constitutional concerns associated with them. And significantly, they all pre-date the Supreme Court’s landmark decision in *Carpenter v. United States*, issued on June 22, 2018.[[18]](#footnote-18)

*Carpenter* makes it clear that individuals have a Fourth Amendment expectation of privacy in their cell phone location data. 138 S. Ct. at 2217. And “[a]llowing government access to cell-site records contravenes that expectation,” even though the information is held by third-party wireless service providers. *Id.* That is because “the time-stamped 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” – the “privacies of life.” *Id.* (internal quotes omitted).

By comparison, accessing cell phone data is “remarkably easy, cheap, and efficient compared to traditional investigative tools.” *Id.* at 2218. With the click of a button, the government “achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.” *Id.* The “retrospective quality” of historical cell site records can also function as a virtual time machine, giving police “access to a category of information otherwise unknowable.” *Id.* And because cell phones are so pervasive, “this newfound tracking capacity runs against everyone.” *Id.*

Accordingly, when the government obtained CSLI in this case through nine tower dumps, it invaded the reasonable expectation of privacy of every cell phone user caught up in the sweep. *See* *Owsley Opinion I*, 930 F. Supp. 2d at 702 (tower dumps are “a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment.”).

The *Carpenter* Court did not decide the constitutionality of tower dumps, but it did recognize that the issues are closely related. 138 S. Ct. at 2220. The difference is that tower dumps intentionally collect private data from hundreds or thousands of non-suspects, as opposed to an individual suspect under investigation. The records contain the same type of CSLI at issue in *Carpenter* as well as other transactional and subscriber data. Apart from the scale and absence of individualized suspicion, there is no logical reason to treat tower dump records different than the CSLI in *Carpenter*. If anything, tower dumps raise greater Fourth Amendment concerns than the individual tracking in *Carpenter*. While their duration may be more circumscribed, their breadth is unlimited, potentially ensnaring thousands of innocent people.

A handful of cases, all decided before *Carpenter*, found that tower dumps are not searches under the Fourth Amendment because users convey their CSLI to wireless service providers. Under the so-called “third-party doctrine” established in the 1970s by *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), there can be no reasonable expectation of privacy in information that is knowingly and voluntarily revealed to such “third parties.” And as a result, some courts felt bound by precedent to permit tower dumps without a warrant and probable cause. *See, e.g., In re Application*, 42 F. Supp. 3d 511, 518 (S.D.N.Y. 2014) (“I agree that Smith and Miller dictate the outcome here, where the subscribers are aware that use of their cell phones necessitates disclosure of the information sought.”); *In re Application*, 2017 WL 6368665, at \*2 (E.D. Mich. Dec. 12, 2017) (“[U]ntil the Supreme Court holds otherwise, I accept that the information the government seeks in this application may be produced under the SCA.”). In a post-*Carpenter* world, however, no court has ruled on the constitutionality of a warrantless tower dump.On the contrary, *Carpenter* dictates that that the third-party doctrine does not apply to CSLI. The Supreme Court explicitly declined to extend *Smith* and *Miller* to these “novel circumstances” in light of the “unique nature of cell phone records,” holding that “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.” *Carpenter*, 138 S. Ct. at 2217.

The Fourth Amendment concerns implicated by *Carpenter* are equally present in this case. The privacy interest in CSLI does not diminish when obtained via tower dump. In both cases, the issue is the government’s ability to use cell site records to locate cell phone users on any given day at any given time, subject only to the data retention policies of wireless carriers. And in both cases, acquisition of the records is a search.

Following *Carpenter*, the government should have obtained a warrant supported by probable cause before obtaining tower dump records. 138 S. Ct. at 2221. Instead, the government used a § 2703(d) order, which requires only “reasonable grounds” for believing that the records were “relevant and material to an ongoing investigation.” 18 U.S.C. § 2703(d). As the *Carpenter* Court explains, “[t]hat showing falls well short of the probable cause required for a warrant” and would be a “‘gigantic’ departure from the probable cause rule.” *Id.* “Consequently,” the Court held, “an order issued under Section 2703(d) of the [SCA] is not a permissible mechanism for accessing historical cell-site records.”

As the Supreme Court has repeatedly noted, “the warrant requirement is ‘an important working part of our machinery of government,’ not merely ‘an inconvenience to be somehow “weighed” against the claims of police efficiency.’” *Riley,* 134 S. Ct. at 2493 (quoting *Coolidge v. New Hampshire,* 403 U.S. 443, 481 (1971)). Where, as here, the data available to law enforcement can reveal personal and private information, not just about a person's whereabouts over time, “but also [about] the people and groups they choose to affiliate with and when they actually do so,” *State v. Earls,* 70 A.3d 630, 642 (N.J. 2013), a warrant should be required. “Before compelling a wireless carrier to turn over a subscriber’s CSLI, the Government’s obligation is a familiar one – get a warrant.” *Carpenter*, 128 S. Ct. at 2221.

**Conclusion**

The government failed to get a warrant for nine tower dumps requesting records from five difference wireless carriers, obtaining the private cell phone records for an unknown number of individuals in Lee County, North Carolina. Instead, the government obtained the records using a provision in the SCA that plainly does not authorize tower dumps. Indeed, tower dumps likely run afoul of the Fourth Amendment altogether to the extent they function as prohibited general warrants. But in light of the Supreme Court’s recent decision in *Carpenter*, the Fourth Amendment demands no less than a warrant based on probable cause to obtain cell site data through a tower dump. The government’s failure to do so here thus requires suppression of the tower dump records and their fruits under the Fourth Amendment, Article I, § 20 of the North Carolina State Constitution; and North Carolina General Statute 15A-974.

**WHEREFORE,** the Defendant respectfully prays unto his Honorable Court for the following relief:

1. Enter an order suppressing the tower dump records obtained by the government; and
2. Redactions of any interview videos of references to the results of the tower dump records; and
3. For any other and further relief to which the Defendant may be entitled and which the Court may deem just and proper.

Respectfully submitted this the 18th day of September, 2018.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Emmanuel Sanders, Pro Se

STATE OF NORTH CAROLINA IN THE GENERAL COURT OF JUSTICE

LEE COUNTY SUPERIOR COURT DIVISION

STATE OF NORTH CAROLINA ) FILE NOs. 14CRS 53533A

) 15CRS 00061A

v. ) 17CRS 00206A

)

EMMANUEL SANDERS )

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

AFFIDAVIT OF STANDBY COUNSEL IN SUPPORT OF MOTION TO SUPPRESS TOWER DUMP RECORDS

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**NOW COMES** Kellie Mannette, standby counsel for Emmanuel Sanders, and being first duly sworn and deposed, says:

1. The sources of information in this affidavit are discovery provided by the state and undersigned’s investigation of this matter.
2. The Defendant is charged with first degree murder, robbery with a dangerous weapon, first degree kidnapping, conspiracy to commit robbery with a dangerous weapon, first degree burglary, and conspiracy to commit burglary. The date of the alleged offense is November 22, 2013. The alleged murder victim is Andy Giles.
3. At about 5:30am on 11/22/13, a “6’ tall black male, in his 20-30’s with shoulder length long braids (pulled back), who was around 225 pounds” broke into the trailer located at 69 Hickory Nut Ct.
4. The man said, “Sheriff’s Department, get on the ground.” The man was wearing a sweatshirt that said, “Sheriff’s Department” and was holding a rifle. The man order Marjorie and Mr. Giles to get on the ground, and when Mr. Giles moved towards him the man shot Mr. Giles. The man shot Mr. Giles. The man then asked where “the money” was, and Mrs. Giles showed him the money. The man then told Mrs. Giles to lay down and he zip tied her feet together. Mr. Giles died from his injuries.
5. The Giles’ called 911 at 5:48am.
6. Officers from the Lee County Sheriff’s Department (LCSO) responded to the scene. They took statements from Mrs. Giles and her two teenaged children, who had also been present.
7. Mrs. Giles reported that while the man was in the home, he spoke to someone on a cell phone.
8. Detective Shawn Ellerby led the ensuing investigation.
9. On 22 November 2013, Detective Ellerby obtained an order compelling “any and all electronic communications providers” to provide “any and all transactional records pertaining to cellular telephone calls, SMS texts, evolution data optimized (EVDO) information, per call measurement data (PCMD) and direct connect information, received by or transmitted from cellular towers… that may provide service to the area in and around 69 Hickory Nut Court, Sanford, N.C.”
10. The time frame covered by this order was from 5:00pm to 6:00am on 22 November 2013.
11. On 26 November 2013, Detective Ellerby notified U.S. Cellular, one of the carriers who had a tower servicing the location of the crime scene, that the order was incorrect and he was seeking records from 5:00am through 6:00am on 22 November 2013.
12. On 5 December 2013, Detective Ellerby obtained a corrected order with identical language but modifying the timeframe to 5:00am through 6:00am on 22 November 2013.
13. A total of 9 cell phone towers from 5 different providers ultimately provided records pursuant to the order. These records are commonly referred to as “tower dump records.”
14. Of the five carriers who provided records, one appeared to attempt to respond to the initial time frame. US Cellular provided tower dump records from 12:00:01am on 22 November 2013 through 11:59:59pm on 22 November 2013. Therefore, instead of the 22 call records that would have been responsive to the intended timeframe, 5,764 call records were provided.
15. Copies of both orders are attached to this motion.
16. In discovery, police associated several numbers found on these tower dump records with people of interest in this case. Phone numbers associated with two of the original co-defendants appeared in the tower dump records. A number associated with current co-defendant Harley Chavis and a number associated with current co-defendant Derek Strickland were found in the tower dump records.
17. There was also a phone number, 919- XXX-XXXX, that was registered to a Johnathan Oakley. Johnathan Oakley was a friend of Chavis, Mintz, and Strickland. He was also Mr. Sanders’ neighbor at one point in time.
18. 919- XXX-XXXX appears on 2 of the tower dumps as receiving several calls between 5:42am and 5:55am.
19. On 29 August 2018, the State provided discovery that Johnathan Oakley had given another interview on 21 August 2018. In that interview, he stated that 919- XXX-XXXX belonged to Mr. Sanders and Mr. Oakley added the number to his phone plan.
20. This is the only notation in discovery that 919- XXX-XXXX was Mr. Sanders’ cell phone number.

**FURTHER AFFIANT SAYETH NAUGHT.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Kellie Mannette

Sworn and subscribed to before me this the \_\_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 2018.

Notary Public: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

My commission expires: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing has been served on the prosecutor by personal service or by leaving a copy of said motion with an employee of the Office of the District Attorney or by United States mail, first class postage paid.

This 19th day of June, 2018.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Emmanuel Sanders, Pro Se

1. Interview with Marjorie Giles, 11/22/13. [↑](#footnote-ref-1)
2. Lee Rainie, et al., Pew Research Ctr., *The Web at 25 in the U.S.* 14 (2014), *available at*

   http://www.pewinternet.org/files/2014/02/PIP\_25th-anniversary-of-the-Web\_0227141.pdf. [↑](#footnote-ref-2)
3. *See Mobile Fact Sheet*, Pew Research Center (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/; *2013 Mobile Consumer Habits Study* 2–3, Harris Interactive (June 2013), http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf [↑](#footnote-ref-3)
4. *See* Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary, 113th Cong. 50, at 6, 9 (2013) (written testimony of Professor Matt Blaze, University of Pennsylvania) (“2013 Blaze Testimony”), available at https://judiciary.house.gov/wp-content/uploads/2016/02/BlazeTestimony.pdf. [↑](#footnote-ref-4)
5. *Id.* [↑](#footnote-ref-5)
6. *See* CTIA—The Wireless Association, *Annual Year-End 2016 Top-Line Survey Results* 4 (May 2017) (308,334 cell sites in 2016). [↑](#footnote-ref-6)
7. A different estimate reports 690,046 towers and 1,954,720 antennae—including those used for cellular and other communications services—as of September 14, 2018. AntennaSearch.com, http://antennasearch.com. [↑](#footnote-ref-7)
8. *Mobile Fact Sheet*, Pew Research Center; CTIA 2016 Survey at 2 (262 million smartphones in use in 2016). [↑](#footnote-ref-8)
9. *See A Peek Inside the GTalkService Connection* (June 28, 2010), https://jon.oberheide.org/blog/2010/06/28/a-peek-inside-the-gtalkservice-connection/ (“In short, the GTalkService is a persistent connection maintained from your Android phone to Google’s servers at all time. It allows Google to push down messages to your phone in order to perform particular actions.”). [↑](#footnote-ref-9)
10. *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1014 (N.D. Cal. 2015) (quoting Declaration of FBI Special Agent Hector M. Luna). [↑](#footnote-ref-10)
11. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 703 (2011). [↑](#footnote-ref-11)
12. Ellen Nakashima, *Agencies Collected Data on Americans’ Cellphone Use in Thousands of ‘Tower Dumps,’*

    Wash. Post, Dec. 8, 2013, http://www.washingtonpost.com/world/national-security/agencies-collected-data-onamericans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed\_story.html (“[E]ach [tower dump] request to a phone company yield[ed] hundreds or thousands of

    phone number of innocent Americans.”). [↑](#footnote-ref-12)
13. *Id.* [↑](#footnote-ref-13)
14. John Kelly, *Cellphone Data Spying: It’s Not Just the NSA*, USA Today, Dec.8, 2013, https://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/. [↑](#footnote-ref-14)
15. The Dictionary Act does not compel a different result. Cf. *In re Cell Tower Records Under 18 U.S.C. 2703(D)*, 90 F. Supp. 3d 673, 676–77 (S.D. Tex. 2015); *In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless*, 42 F. Supp. 3d 511, 513 (S.D.N.Y. 2014). Under the Act, “words importing the singular include and apply to several persons, parties, or things” – “*unless* the context indicates otherwise.” 1 U.S.C. § 1 (emphasis added). Here, the context indicates otherwise. [↑](#footnote-ref-15)
16. The harms here are not speculative. In addition to Mr. Sanders, six other individuals were arrested for the crimes alleged in this case based on the tower dump data obtained by the government. The charges against these six individuals were dismissed after 10 months, presumably because the government determined through other means that they were not responsible and had been wrongly charged and detained. [↑](#footnote-ref-16)
17. *See, e.g.,* Hon. Brian L. Owsley, *The Fourth Amendment Implications of the Government’s Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. Pa. J. Const. L. 1, 17–23 (2013) (law enforcement agencies use tower dumps “routinely”); Verizon, Transparency Report 1H 2017, https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2018/05/Transparency-Report-US-1H-2017.pdf (reporting approximately 8,870 warrants or court orders for “cell tower dumps” in the first half of 2017). [↑](#footnote-ref-17)
18. *See In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d) Directing Providers to Provide Historical Cell Site Locations Records* (“ Owsley Opinion I”), 930 F. Supp. 2d 698 (S.D. Tex. 2012) (Owsley, M.J.); *In re Search of Cellular Phone Towers* (“ Owsley Opinion II”), 945 F. Supp. 2d 769, 770 (S.D. Tex. 2013) (Owsley, M.J.); *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)* (“Owsley Opinion III”), 964 F. Supp. 2d 674 (S.D. Tex. 2013) (Owsley, M.J.); *In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. §§ 2703(c) and 2703(d)*, 42 F.Supp.3d 511 (S.D.N.Y.2014); *United States v. Pembrook,* 119 F.Supp.3d 577 (E.D. Mich. 2015); *In re Cell Tower Records Under 18 U.S.C. 2703(D)*, 90 F. Supp. 3d 673, 675 (S.D. Tex. 2015); *In re Application of the United States for an Order Pursuant To 18 U.S.C. §2703(d)*, No. 2:17-MC-51662, 2017 WL 6368665 (E.D. Mich. Dec. 12, 2017). [↑](#footnote-ref-18)