

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

UNITED STATES OF AMERICA,)	
)	
)	
v.)	Criminal Action No.
)	1:17-CR-315-LMM-JKL
)	
DONTIEZ PENDERGRASS, et al.)	
Defendant.)	

**Defendant’s Motion to Suppress Evidence Evidence as a Result of the Tower
Dump in the Instant Case.**

COMES NOW THE DEFENDANT, by his undersigned counsel, to move this Court to allow this out of time motion to suppress and shows the following.

Background.

Mr. Pendergrass and his codefendant were indicted by the grand jury in September, 2017, and charged with five Hobbs Act robberies and five violations of 18 U.S.C. §924(c), exposing them to a potential sentence of life (see §924(c)) along with minimum sentences with potential exposure of more than 100 years. While this matter is set for trial in June, 2019, counsel has continued to prepare a trial defense for Mr. Pendergrass and has continued to explore all avenues to his benefit. Last week, counsel was made aware of a recent article in the Champion Magazine (NACDL, Feb. 2019) regarding “tower dumps” and their relationship to

Carpenter v. United States, 138 S. Ct. 2206 (2018). Because of the Fourth Amendment concerns the tower dumps in this case pose to Mr. Pendergrass and his potential exposure, counsel believes it prudent to bring this motion at this time.

Relevant Facts.

As stated earlier, the defendants are charged in a multi-count indictment alleging robberies occurring on November 19, 2016, December 24, 2016, January 1, 2017, January 5, 2017, and January 15, 2017, in Gwinnett County, Georgia. The government sought and received an order for a “tower dump” on or about January 30, 2017 as part of its investigation. Said order required that the requested carriers provide a swath of information regarding the phone users that may or may not have been in the geographical area of the robbery.¹

A tower dump “pull[s] in the phone numbers and [proximate] location of everyone in the vicinity of the event.” Nate Anderson, “*How Cell Tower Dumps Caught the High Country Bandits—and Why It Matters*,” *Ars Technica*, Aug. 29, 2013, <https://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters/>. The tower dump provides the government with a record of every individual that was near a cell tower, or group of cell towers, during a given time period. These searches invade the privacy of not just one individual, but potentially thousands. Tower dump records are at least as

¹ Both the Application and the Order are attached as Exhibits 1 and 2, respectively.

“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.)). As a result, this Court should suppress all tower dump records obtained without a warrant, and all of the fruits thereof.

In 2014, Gwinnett County had a population of 808,374,² and had a population density of almost 1851 people per square mile in some areas, and so a tower dump like that ordered in this case could easily cover as many as 10,000 people. Smartphones connect to cell sites without users having to interact with the device at all. *See Carpenter*, 138 S.Ct. at 2220 (“[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up”). Tower dump requests therefore reveal increasingly large and precise amounts of location data as even more Americans switch to smartphones, and as improved technology permits cell phones to connect with towers at an even faster speed. 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

² See Exhibit 3, Gwinnett County Population, <https://population.us/county/ga/gwinnett-county/>.

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*.

Again, the government should have obtained a 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.

ARGUMENT

A. A Tower Dump Is a “Search” Under the Fourth Amendment.

The Supreme Court recently held in *Carpenter* that individuals have a reasonable expectation of privacy in their cell phone location data, and that the government’s acquisition of those records from the defendant’s cellular service provider in that case was a Fourth Amendment search. 138 S. Ct. at 2217. This holding must apply with equal force in the context of a tower dump request because of the personal information gathered by the cell phone carriers. Whether this Court analyzes this claim under the reasonable expectation of privacy framework set forth in *Katz v. United States*, 389 U.S. 347 or a property-based theory of law, it should reach the same conclusion that tower dump is a search under the Fourth Amendment.

1. Users Have a Reasonable Expectation of Privacy in Their Cell Phone Location Data.

In considering whether citizens reasonably expect information to remain private, the Supreme Court has crafted “a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also Carpenter*, 138 S. Ct. at 2213, 2217 (applying the *Katz* analysis in the context of CSLI and concluding that users have a reasonable expectation of privacy in this information). For reasons discussed below, the defendant has evinced both a subjective and objective expectation of privacy, and therefore a tower dump is a Fourth Amendment search.

Although the Court did not rule on the constitutionality of tower dumps in *Carpenter*, 138 S. Ct. at 2220, the Court’s rationales for concluding that users have a reasonable expectation of privacy in their long-term CSLI apply with equal force to the cell phone location information received from a tower dump. In *Carpenter*, the Court explained that “the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection” give rise to a reasonable expectation of privacy. *Id.* at 2223. These

factors are equally relevant when the government collects CSLI through a tower dump, and should similarly demand Fourth Amendment protection.

In addition, the third-party doctrine does not apply to cell phone location information collected during a tower dump. In *Carpenter*, the Court held that the third-party doctrine could not apply to cell-site location information because “the nature of the particular documents sought” were highly “revealing” and because users did not “voluntarily” share that information with the third-party. *See Carpenter* at 2219–20. The cell-site location information collected pursuant to a tower dump is similar in both respects.

Tower dumps reveal information about constitutionally protected spaces such as the home—which is “presumptively unreasonable in the absence of a search warrant.” *Katz*, 389 U.S. at 361. Cell phone location data is precise; it can be used to locate someone “not only around town but also within a particular building.” *Riley v. California*, 134 S.Ct. 2473, 2490 (2014). A tower dump will provide a time-stamped CSLI of the device wherever the user carried it. Because “individuals . . . compulsively carry cell phones with them all the time,” *Carpenter*, 138 S.Ct. at 2218, users will carry their devices with them within their homes. Because a tower dump gathers the CSLI of multiple users—up to thousands—at a time, the risk that a tower dump will reveal the precise location information of at least one individual within her home is high. The Court has

repeatedly emphasized that “the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion” is at the very heart of the Fourth Amendment. *Silverman v. United States*, 365 U.S. 505, 511 (1961); *Kyllo v. United States*, 533 U.S. 27, 37 (2001); *Knotts*, 460 U.S. at 282 ; *United States v. Karo*, 468 U.S. 705, 715 (1984). The sanctity of the home was assured at the time of the adoption of the Fourth Amendment, and the Court has long expressed concern with establishing “what limits there are upon this power of technology to shrink the realm of guaranteed privacy.” *Kyllo*, 533 U.S. at 34. A tower dump is far too expansive an invasion of the “sanctity of the home” or any other constitutionally protected area. *Id.* at 37.

Cell phone information gleaned from a tower dump can also reveal private facts about protected activities and other intimate spaces, violating an individual’s reasonable expectation of privacy. In *Carpenter*, the Court acknowledged this potential, noting: “A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *Carpenter*, 138 S.Ct. at 2218. As one amicus brief in *Carpenter* noted, a tower dump of a cell site near an 8:30 pm Alcoholics Anonymous meeting “will reveal all the devices—and therefore individuals—in that meeting. . . . The same conclusions hold for other sensitive and protected associational activities—including religious evangelism, student

activism, and union organizing.” *Brief of Technology Experts as Amici Curiae in Support of Petitioner* at 35-36, *Carpenter, supra*. Another amicus brief in *Carpenter* observed that “[d]ue to the ubiquitous nature of cell phones, location information gleaned from cell towers can disclose an individual’s expressive and associational activities such as “a journalist’s newsgathering process.” *Brief of The Reporters Committee for Freedom of the Press and 19 Media Organizations as Amici Curiae in Support of Petitioner* at 10, *Carpenter, supra*. These briefs expressed fears that CSLI can reveal information not only about intimate and constitutionally protected spaces, but also infringe on First Amendment activities. *See United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (“Awareness that the Government may be watching chills associational and expressive freedoms”). By revealing information about constitutionally protected spaces and protected activities, tower dumps have precisely the pernicious effect on an individual’s realm of privacy that the Court has held violates the Fourth Amendment. *See, e.g., Kyllo*, 533 U.S. at 40.

2. A Tower Dump is More Comprehensive and Broad Than a Traditional Location Tracking Because It Can Construct Location Retroactively.

A tower dump request intrudes on a reasonable expectation of privacy based on the historical location information it provides. The Court has held that

individuals cannot reasonably expect to remain unobserved in public spaces: in *Knotts*, the Court held that surveillance of an automobile traveling on public streets did not violate a reasonable expectation of privacy, since “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” 460 U.S. 276, 281 (1983). Yet the Court was careful to note in *Carpenter* that “[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere.” 138 S.Ct. at 2217. The *Carpenter* majority observed that, unlike the beeper used to track location in *Knotts*, “the retrospective quality of the data here gives police access to a category of information otherwise unknowable. . . . With access to CSLI, the government can now travel back in time to retrace a person’s whereabouts.” *Id.* at 2218. This retrospective quality distinguishes long-term CSLI as well as tower dumps from the real time, simple tracking at issue in *Knotts*, which “amounted principally to the following of an automobile on public streets and highways.” 460 U.S. at 281. Tower dump location information reveals more than what would otherwise be publicly observable, because an individual’s location is constructed retroactively; therefore, this method of surveillance is categorically different from the simple beeper used in *Knotts*, which merely replaced plain view surveillance. *Carpenter*, 138 S.Ct. at 2220–21; *see also Prince Jones*, 168 A.3d at 712 (citing *Knotts*, 460 U.S. at 282) (“But although the kind of device used in *Knotts* and *Karo*

is probably more reliable than a human tracker—less prone to discovery than a human and harder to elude—at their core these devices merely enable police officers to accomplish the same task that they could have accomplished through ‘[v]isual surveillance from public places.’”).

Because a single tower dump request reveals a multitude of users’ cell phone location information, a tower dump permits the government to retroactively locate hundreds or thousands of individuals at almost no cost, reconstructing a complete picture of who was in a given location at a given time. The government has never had such comprehensive surveillance abilities, and §2703(d) order should not be the only barrier to such a pervasive surveillance technique.

At the time of the adoption of the Fourth Amendment, retrospective reconstruction of an individual’s movements would have been impossible, a concern which animated the holding in *Carpenter*. As the Court in *Carpenter* explained: “As technology has enhanced the government’s ability to encroach upon areas normally guarded from inquisitive eyes,” courts “must ‘assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” 138 S.Ct. at 2214 (quoting *Kyllo v. United States*, 533 U. S. 27, 34 (2001)). Warrantless tower dump requests therefore impermissibly “shrink the. . . realm of privacy” guaranteed by the Fourth Amendment. *Kyllo*, 533 U.S. at 32, 40 (holding that where the use of sense-

enhancing technology to search a constitutionally protected space violated a reasonable expectation of privacy since the information “would previously have been unknowable without physical intrusion.”); *see also Prince Jones*, 168 A.3d at 714 (citing *Maryland v. Andrews*, 134 A.3d 324, 348 (Md. App. 2016) (holding that the use of a cell-site simulator without a warrant violated the Fourth Amendment because “[u]nlike in a situation in which the government determines a person’s location through visual surveillance or by employing the older generation of tracking devices, it cannot be argued that ‘the information obtained by [the government] in this case was . . . readily available and in the public view’”) (internal citations omitted). Based on their potential to reconstruct an individual’s historical movements and reveal sensitive information and activities, tower dumps categorically violate a reasonable expectation of privacy.

3. The Third-Party Doctrine Should Not Apply to Data Collected by a Tower Dump Because the Collection of CSLI is Inescapable and Automatic.

In *Carpenter*, the Court rejected the government’s argument that the third-party doctrine applied to CSLI. The Court provided two main rationales for this decision: that CSLI is particularly revealing in nature and qualitatively different from types of business records to which the doctrine may apply, and that users do

not voluntarily share their cell-site location information. *See id.* at 2219–20. These two rationales apply with equal force to a tower dump search.

Cell-site records are qualitatively different from the business records to which the third-party doctrine traditionally applies. In *Smith v. Maryland*, the Court held that a user did not have a reasonable expectation of privacy in numbers that he had dialed on a landline and shared with a telephone operator. 442 U.S. 735, 742. In *United States v. Miller*, the Court reached the same conclusion, holding that individuals did not have a reasonable expectation of privacy in bank statements and deposit slips that were shared with a bank teller. 425 U.S. 435, 440 (1976). Although tower dumps similarly concern the government’s collection of telephone numbers, the records here are very different from the records collected by the pen register used in *Smith*. *See Carpenter*, 138 S. Ct. at 2219 (comparing CSLI to “the limited capabilities of a pen register”).

First, *Smith* involved a “one-time, targeted request for data regarding an individual suspect in a criminal investigation.” *Klayman v. Obama*, 957 F. Supp. 2d 1, 33 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015). A tower dump, in comparison, is neither a targeted search nor a narrow search of one individual. Instead, it is utilized by law enforcement because they cannot identify the name or identity of an individual suspect, and implicates hundreds, if not thousands, of individuals in the process.

Second, a pen register reveals only the telephone numbers that an individual dialed. *Carpenter*, 138 S.Ct. at 2216 (citing *Smith*, 442 U.S. at 742)). In comparison, a tower dump reveals not only a chronological list of telephone numbers, but also the cell phone's approximate location. Location information can provide a wealth of "identifying information," *Riley*, 134 S.Ct. at 2493, if, for example, a cell tower is located near a church, doctor's office, or political headquarters. *See also* Hon. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 J. of Const. L. 1, 17 (2013) (citations omitted) (noting that "the government routinely requests more information than just the telephone numbers dialed" when it seeks a tower dump order.).

Individuals do not voluntarily share their location information with their cell-phone provider, further supporting the notion that third-party doctrine is inapposite in this context. The third-party doctrine is justified by the assumption that an individual cannot reasonably expect "information he voluntarily turns over to third parties" to remain private. *Smith*, 442 U.S. at 44. In *Carpenter*, the Court emphasized that cell phone users' "sharing" of their location data with their service provider is not done on a voluntary basis: "Cell phone location information is not truly 'shared' as one normally understands the term. In the first place, cell phones and the services they provide are 'such a pervasive and insistent part of daily life'

that carrying one is indispensable to participation in modern society.” 138 S.Ct. at 2220 (quoting *Riley*, 134 S.Ct. at 2484). Moreover, “a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up.” *Carpenter*, 138 S.Ct. at 2220. The only way an individual could avoid “sharing” their cell phone location data would be to “disconnect[] the phone from the network” altogether, rendering it useless as a communication device. *Id.* It cannot be that by choosing to “participat[e] in modern society” and merely carrying a cell phone which is switched on, an individual relinquishes any expectation of privacy in their location information. *Id.*

4. CSLI is Property That Is Protected by the Fourth Amendment’s Prohibition Against Unreasonable Searches and Seizures.

Under a property-based theory of the Fourth Amendment, defendant’s location data constitutes [his/her] “papers or effects,” whether or not they are held by a third-party cell phone provider, and thus cannot be searched or seized without a warrant. *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting). In his opinion in *Carpenter*, Justice Gorsuch argued that under a “traditional approach” to the Fourth Amendment, the protection against unreasonable searches and seizures applied as long as “a house, paper or effect was yours under law.” *Id.* at 2267–68 (Gorsuch, J., dissenting); *see also Florida v. Jardines*, 569 U.S. 1, 5 (2013) (citing *United States v. Jones*, 565 U.S. 400, 406 n.3 (2012)) (“The Amendment

establishes a simple baseline, one that for much of our history formed the exclusive basis for its protections: When ‘the Government obtains information by physically intruding’ on persons, houses, papers, or effects, ‘a search’ within the original meaning of the Fourth Amendment ‘undoubtedly occurred’”). Justice Gorsuch drew a strong analogy to mailed letters, in which people have had an established Fourth Amendment property interests for over a century, whether or not these letters are held by the post office. *Id.* at 2269 (citing *Ex parte Jackson*, 96 U.S. 727, 733 (1877)). Just as individuals retain property interests in letters in transit while the letters are in the physical possession of a post office, cell phone users have property interests in their location data even when it is stored by cell phone service providers. As Justice Gorsuch explained, private and sensitive records in the hands of a third party can fall under the Fourth Amendment’s protection of a person’s “papers” even when control of and proprietary interest in those records is divided between the individual to whom they pertain (i.e., Defendant) and the business with custody of them (i.e., the cellular service provider). 138 S. Ct. at 2268–69. Where “positive law” allocates at least some property rights in third-party-held data to an individual, the Fourth Amendment’s protections apply. *Id.* at 2270.

Here, cell phone location information is specifically protected by law. The federal Telecommunications Act requires “express prior authorization” of the

customer before a service provider can “use or disclose . . . call location information,” which the law categorizes as “customer proprietary information.” 47 U.S.C. § 222(f). The statute therefore grants users substantial legal interests in this information, including at least some right to include, exclude, and control its use.” *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting). If location data generated by a cell phone constitutes the user’s property, then its seizure and search by the government without a warrant violates the Fourth Amendment. *See also Riley v. California*, 134 S. Ct. 2473, 2490 (holding Fourth Amendment applies to information contained on a cell phone *and* associated information “stored on remote servers” since “[c]ell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.”).

5. A Tower Dump Is a Dragnet Search Forbidden by the Fourth Amendment Because It is Akin to a General Warrant.

Tower dumps are the epitome of the “dragnet-type law enforcement practice[]” that the Court feared in *Knotts*, 460 U.S. at 284, sweeping up the location data of up to thousands of innocent individuals in the hopes of finding one potential lead. The Court has always been “careful to distinguish between [] rudimentary tracking . . . and more sweeping modes of surveillance,” in deciding whether a search is entitled to heightened protection under the Fourth Amendment.

Carpenter, 138 S.Ct. at 2215 (citing *Knotts*, 460 U.S. at 284), and tower dumps fall on the “sweeping” end of this spectrum.

The dragnet nature of a tower dump is illuminated by a comparison to the “rudimentary tracking” conducted in the beeper cases such as *Knotts* and *Jones*. In these cases, the government only sought to track *one* individual. To do so, law enforcement first needed to identify the individual, and then to physically install a tracking device on an object that was in their possession. A tower dump removes the investigative steps that were critical in both *Knotts* and *Jones*: The government no longer needs to know who the target is, and “[w]ith 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; *see also United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) (“Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive”).

Tower dump information can be even more invasive and pose a heightened threat to privacy compared to a single individual’s historical CSLI. While the collection of an individual’s CSLI risks tracking him or her in a private or constitutionally protected area, a tower dump of an area near “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, [or] the gay bar”

can allow the government to piece together a comprehensive overview of *every* attendee in such a space. *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring) (quoting *People v. Weaver*, 909 N.E.2d 1195, 1999 (N.Y. 2009)). While the Court has already expressed concern about creating a “comprehensive record of a person’s public movements,” *Riley* 134 S. Ct. at 2490 (citing *Jones*, 565 U.S. at 415), a tower dump raises a parallel concern—creating a comprehensive record of all individuals at a given location. At issue is not only the government’s ability to “ascertain, more or less at will, [an individual’s] political and religious beliefs, sexual habits, and so on,” *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); it is their ability to do so for hundreds or thousands of individuals.

The dragnet quality of the search is compounded by the fact that once the tower dump is completed, the government can use “the most advanced twenty-first century tools, allowing it to ‘store such records and efficiently mine them for information years into the future,’” creating a risk of repeated surveillance. *Klayman*, 957 F. Supp. 2d at 33 (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)); *see also Comprehensive Drug Testing*, 621 F.3d 1162, 1175 (9th Cir. 2010) (en banc) (per curiam) (remarking that “the threat to the privacy of innocent parties from a vigorous criminal investigation” is heightened when sensitive data of multiple individuals is intermingled in electronic storage.). If the Court previously feared “the Government’s unconstrained power to assemble data that

reveal private aspects of identity is susceptible to abuse” with just one individual, *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring), that fear is compounded by the multitude of persons captured by a tower dump. Based on its capacity to reveal sensitive information about countless individuals, a tower dump is the hallmark of a “dragnet search.” *See Carpenter*, 138 S.Ct. at 2267 (Gorsuch, J., dissenting).

Although the technology is relatively new, an order under 18 U.S.C. § 2703(d) for tower dump records is simply the modern-day equivalent of searching every home in a several-block radius of a reported gunshot, or searching the bags of every person walking along Broadway because of a theft in Times Square. As 2703(d) orders are no longer valid under *Carpenter*, without even the name or number of a potential target, law enforcement can search the CSLI of all individuals, merely due to their proximity to the unknown suspect. *Cf. Sibron v. New York*, 392 U.S. 40, 63–64 (1968) (holding that “[t]he suspect’s mere act of talking with a number of known narcotics addicts over an eight-hour period” did not give rise to neither reasonable suspicion nor probable cause to search him). Tower dump orders harken back to the “writs of assistance” that permitted “British officers to rummage through homes in an unrestrained search for evidence of criminal activity;” searches that “helped spark the Revolution itself.” *Riley*, 134 S.Ct. at 2494; *Carpenter*, 138 S.Ct. at 2213 (citing *Riley*, 134 S.Ct. at 2494). This type of “exploratory rummaging” is the provenance of prohibited general warrants

and thus forbidden by the Fourth Amendment. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). *See also Wilkes v. Wood*, 98 Eng. Rep. 489, 498 (1763) (condemning a search where the “discretionary power [was] given to messengers to search wherever their suspicions may chance to fall”); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding that a “warrant to search all suspected places [for stolen goods]” was unlawful because “every citizen of the United States within the jurisdiction of the justice to try for theft, was liable to be arrested”).

Even the “reviled general warrants and writs of assistance of the colonial era,” *Riley*, 134 S.Ct. at 2494, were subject to the practical constraints posed by “limited police resources and community hostility.” *Illinois v. Lidster*, 540 U.S. 419, 426 (2004). This is not so with tower dumps. Individuals will not be alerted when law enforcement officials have obtained their cell-site location data, The Honorable 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, 46 (2013), and the government can receive this information at little to no cost. *See Carpenter*, 138 S.Ct. at 2218 (noting that the government can access “historical location information at practically no expense”). This makes a tower dump all the more dangerous and risks “alter[ing] the relationship between citizen and government in a way that is inimical to democratic society.” *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

These concerns are amplified as the government increasingly turns to tower dumps as an initial step in an investigation. Katie Bo Williams, *Verizon Reports Spike in government Requests for Cell ‘Tower Dumps’*, The Hill, August 24, 2017, <https://thehill.com/policy/national-security/347800-government-requests-for-cell-tower-dumps-spikes-verizon> (noting that in 2017, Verizon “received approximately 8,870 warrants or court orders for cell tower dumps in the first half of [the] year—a huge increase over 2013, when the government sought only 3,200 dumps In 2016, the total figure was 14,630”); The Honorable 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, 2 (2013) (“[T]he actions by most of the largest cell providers, as well as personal experience and conversations with other magistrate judges, strongly suggest that [tower dumps have] become a relatively routine investigative technique”). Although “the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities,” a tower dump also “risks [g]overnment encroaching of the sort the Framers, ‘after consulting the lessons of history,’ drafted the Fourth Amendment to prevent. *Carpenter*, 138 S.Ct. at 2223 (citing *Di Re*, 332 U.S. 581, 595 (1948)).

6. A Tower Dump is an Unconstitutional Search Under the Fourth Amendment and Suppression of the Tower Dump Records Is Required.

Tower dump requests pose unique risks to the guarantees of the Fourth Amendment: they violate individuals' reasonable expectations of privacy, revealing these individuals' cell phone location information merely because they were in the vicinity of a suspected crime. Tower dumps are impermissible under the Fourth Amendment's prohibition on general warrants, as it would be impossible to establish probable cause to search hundreds of individuals without even a single named suspect. As such, this Court should hold that the government's use of the tower dump records is unconstitutional under the Fourth Amendment.

Tower dumps are exceedingly ill-suited to the relevant and traditional inquiries concerning warrants. It would be impossible to establish the requisite probable cause necessary to gather the cell-site location information of everyone in a given vicinity. *See Ybarra v. Illinois*, 444 U.S. 85, 86 (1979) (noting that "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."). The government would also be unable to "particularly describe the 'things to be seized'" as well as the place to be searched. *Dalia v. United States*, 441 U.S. 238, 255 (1979) (citing *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Although the

government might be able identify the place to be searched in advance of a tower dump request, it cannot state with particularity the individuals it is searching—let alone the name of a single targeted individual or phone number. This fails to meet the particularity requirement of the Fourth Amendment. *See, e.g., Groh v. Ramirez*, 540 U.S. 551, 558 (2004) (noting that the warrant was “deficient in particularity” because “in the space set aside for the description of the items to be seized, the warrant stated that the items consisted of a ‘single dwelling residence . . . blue in color.’ In other words, the warrant did not describe the items to be seized *at all*.”); *cf. United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (noting that there is a “heightened sensitivity to the particularity requirement in the context of digital searches.”). Additionally, the particularity requirement is at its most stringent when items to be seized raise First Amendment concerns, *Stanford*, 379 U.S. at 485. Cell phone location information can show individuals’ presence at religious or political locales, *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring), implicating First Amendment concerns and underscoring the inability for the government to sufficiently particularize in the context of a tower dump. The consequence of the inability to apply these criteria to a tower dump is simple: a warrant cannot authorize one.

However, even if the warrant instrument is capable of authorizing a tower dump, it is clear that a warrant alone (and not legal process requiring a lower

threshold of justification) can do so. The rationale of *Carpenter* makes that much clear. *Carpenter*, 138 S. Ct. at 2221.³ When a search has the potential to sweep up information that does not pertain to the suspect under investigation and is not justified by the government’s showing of probable cause, the court must ensure that the government has taken steps to ensure minimization and particularity of the search. A warrant for tower-dump data could only be valid if—at a minimum—it requires minimization of the amount of innocent third parties’ data collected,⁴

³ Some major telephone companies may in fact already be requiring probable-cause warrants for this type of information. See *United States Report*, Verizon, <https://www.verizon.com/about/portal/transparency-report/us-report/> (“[In *Carpenter*, a] majority of the Court concluded that a warrant was necessary. Since the Court’s ruling, Verizon has accepted only probable cause warrants before releasing historical location information”); *Transparency Report*, AT&T, Aug. 2018, <http://about.att.com/content/dam/csr/aug2018/TransparencyReports/Aug-2018-TransparencyReport.pdf> (“[I]n light of the ruling, we will require a search warrant based on the probable cause standard for all demands for real-time or historical location information, again except in emergency situations”).

⁴ For example, a court should narrow the time period covered by the government’s request. See *In re Search of Cellular Phone Towers* (“Owsley Opinion II”), 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013) (Owsley, M.J.). The length of time covered by a tower dump authorization must be narrowly tailored to the crime under investigation; there must be a nexus between the government’s probable cause showing and the timespan of the request.

restricts retention of such data after the search,⁵ and mandates notice to all persons whose cell phone location information the government has obtained.⁶

Here, instead, the government used a § 2703(d) order under the Stored Communications Act, now outlawed, which requires only “specific and articulable facts showing that there are reasonable grounds” for believing that the records are “relevant and material to an ongoing investigation.” 18 U.S.C. § 2703(d). As the *Carpenter* majority explained, “[t]hat showing falls well short of the probable cause required for a warrant” and allowing it would be a “‘gigantic’ departure from the probable cause rule.” 138 S.Ct. at 2221; *see also 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, 702 (S.D. Tex. 2012) (Owsley, M.J.) (explaining that the “failure to address the privacy rights for the Fourth Amendment concerns of . . . innocent subscribers whose information will be compromised at a request of the cell tower

⁵ As soon as practicable after the government has reviewed the tower dump records, it should be required to “return any and all original records and copies, whether hardcopy or in electronic format or storage, to the Provider, which are determined to be not relevant to the Investigative Agency’s investigation.” *Owsley Opinion II*, 945 F. Supp. 2d at 771.

⁶ Without receiving notice, affected persons—particularly non-suspects—will have no way to learn that they have been subjected to a search and no opportunity to vindicate any violation of their constitutional rights. Notice of a government search is required by Rule 41. *See* Fed. R. Crim. P. 41(f)(1)(C).

dump is another factor warranting the denial” of § 2703(d) order). Consequently, the government’s failure to get a probable-caused based warrant that complies with the Fourth Amendment’s particularity and notice requirements renders the search unconstitutional.

Wherefore, the defendant requests that the Court allow this out of town motion, allow the government sufficient time to respond, should it choose to do so, and grant such further relief as the Court deems necessary and proper.

This 3d day of February, 2019.

Respectfully submitted,

S/R. Gary Spencer
R. GARY SPENCER, ESQ.
STATE BAR NO. 671905
ATTORNEY FOR DONTIEZ
PENDERGRASS

R. GARY SPENCER, P.C.
50 Hurt Plaza, Ste. 830
Atlanta, GA 30303
404-549-8782
1-888-572-1831 (fax)

*Counsel acknowledges assistance from the Fourth Amendment project of the NACDL in this motion.

CERTIFICATE OF SERVICE

I certify that the foregoing reply was placed in the Court's electronic filing system this 3d day of February, 2019, where the parties shall be served electronically.

Respectfully submitted,

S/R. Gary Spencer

R. GARY SPENCER, ESQ.
STATE BAR NO. 671905
ATTORNEY FOR DONTIEZ
PENDERGRASS

R. GARY SPENCER, P.C.
50 Hurt Plaza, Ste. 830
Atlanta, GA 30303
404-549-8782
1-888-572-1831 (fax)