SUPERIOR COURT OF NEW JERSEY,
APPELLATE DIVISION
DOCKET NO.: A-001399-24T2

STATE OF NEW JERSEY, Plaintiff-Respondent, v. **PHILLIP D. BRYANT AND JAMES HUNTER,** Defendants-Appellants.	CRIMINAL ACTION On Leave to Appeal Granted from an Order of the Superior Court of New Jersey, Law Division, Middlesex County. Indictment No.: 22-02-124-I Sat Below Hon. Thomas J. Buck, J.S.C.

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION & AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY

Dillon Reisman (374142021)
Ezra D. Rosenberg (012671974)
Jeanne LoCicero (024052000)
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY FOUNDATION
[redacted]
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
dreisman@aclu-nj.org
erosenberg@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
[redacted]
Tel: (415) 343-0758
jgranick@aclu.org

Attorneys for Amici Curiae
* Pro hac vice pending

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

PRELIMINARY STATEMENT

After only nine days investigating a home break-in, the Middlesex County Prosecutors Office elected the nuclear option: a "tower dump" seeking historical cell site location information (CSLI) and call records of all individuals who made phone calls or texts using several cell phone towers during designated periods of time. This dragnet is a fundamentally new and invasive electronic search technique that evades longstanding practical barriers to sweeping police surveillance. Even data from a single cell tower can reveal presence inside the home or a place of worship, at a protest or political rally, or coming and going from a hospital—not just for one individual, but potentially for *everyone* who used their phone in an expansive area over the specified time period.

In this case, the tower dumps obtained from four cellular providers returned the private information of over ten thousand uninvolved people living within a 193 square mile area, far afield from the single home broken into in South Plainfield. This result is to be expected, because tower dumps are overbroad by their nature. By collecting troves of data about people with no connection to the crime, tower dumps are precisely the sort of "general searches" that the Fourth Amendment and Article I, Paragraph 7 forbid.

This Court's review of the case should be informed by the relationship between tower dumps and general warrants. First, the kind of tower dump obtained in this case failed to meet the Fourth Amendment or Article I, Paragraph 7's safeguards against general warrants. (Point I). Second, tower dumps contain intrusive, detailed information about indiscriminate numbers of people within an entire jurisdiction, which police can seek to use in future investigations without judicial oversight. (Point II). Finally, the use of tower dumps in this case was overbroad, gratuitous, and unaccountable in ways that bear the hallmarks of a general search. (Point III).

To be clear, a proper warrant may authorize law enforcement to access known, specified individuals' cell-site location information and call records. This is the holding of *State v. Earls*, 214 N.J. 564, 589 (2013). But just as a warrant can authorize the search of one person's house but not every house on the block, neither can a tower dump warrant purport to sweep up the activities, associations, and personal lives of hundreds to thousands of people who may have been miles away from a crime scene. That is the essence of a general warrant. To suggest otherwise is a radical expansion of police power past constitutional limits.

For these reasons, Amici ask this Court to rule that tower dump searches are unconstitutional general warrants and to suppress the cell-site location information and call records obtained through the tower dumps.

INTERESTS OF AMICI CURIAE

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The American Civil Liberties Union of New Jersey ("ACLU-NJ") is the New Jersey state affiliate of the national ACLU. For over 60 years, the ACLU-NJ has defended liberty and justice guided by the vision of a fair and equitable New Jersey for all.

Since its founding in 1920, the ACLU has frequently appeared before the U.S. Supreme Court and other state and federal courts in numerous cases implicating Americans' right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 585 U.S. 296 (2018), as amicus (with the ACLU-NJ) in *State v. Missak*, 476 N.J. Super. 302 (App. Div. 2023), and in *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020), *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc), *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The ACLU-NJ has appeared frequently before this Court and the New Jersey Supreme Court advocating for the rights to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article I, Paragraph 7 of the New Jersey Constitution. *See, e.g.*, *State v. Lunsford*, 226 N.J. 129 (2016) (telephone billing and toll records); *State v. Earls*, 214 N.J. 564 (2013) (cell phone location data); *State v. Reid*, 194 N.J. 386 (2008) (Internet service provider subscription information).

Recently, both the ACLU and ACLU-NJ appeared before this Court in *State v. Salter*, A-3963-23T6 (N.J. Super. Ct. App. Div. Dec. 16, 2024), concerning the application of Article I, Paragraph 7 and the Fourth Amendment to "geofence searches", a technique similar to the one here where there is no suspect: law enforcement obtains sensitive location information about multiple people simply because they were near where a crime took place. The instant case raises similar questions to those in *Salter*, both involving the relationship between our constitutional search provisions and novel location-based reverse-search techniques.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

Amici rely on the statement of facts and procedural history found in Defendant's Supplemental Brief.

ARGUMENT

Tower dumps enable the exact kind of "general, exploratory rummaging" that our federal and state constitutions were meant to prevent. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). They effectively give law enforcement a time machine to search indiscriminately through the past lives of people within their entire jurisdiction—for some cellular providers, the police can rewind the clock up to seven years.[1] The Framers would have never contemplated such a thing as possible and would recognize this power as anathema to a free society. Warrants authorizing tower dumps are the kind of "general warrant" that purport to give law enforcement "blanket authority to search where they pleased," violating Article I, Paragraph 7 of the New Jersey Constitution and the Fourth Amendment of the United States Constitution. *State v. Feliciano*, 224 N.J. 351, 366 (2016); *see Riley v. California*, 573 U.S. 373, 403 (2014).

To be clear, law enforcement can use judicial process to access cell-site location information and call records for specific, known individuals. *See State v. Earls*, 214 N.J. 564, 588 (2013). But that ability is limited. Just as a warrant cannot authorize the indiscriminate search of multiple dwellings where police

---

[1] Fed. Bureau of Investigation, CAST, *Cellular Analysis & Geo-Location—Field Resource Guide* (2019), Aa2. Hyperlinks to external resources are available in the appendix's table of contents.

must find probable cause to search only one, tower dump warrants are unconstitutional because they purport to authorize a vast, broad search of constitutionally-protected information, activities, and associations of hundreds to thousands, when police should develop probable cause to track only one or a few people. *See State v. Marshall*, 199 N.J. 602, 616–17 (2009) (finding a warrant to search either of two apartments was invalid where there was "no evidence of any effort by the police to determine" which of the two apartments belonged to the suspect). That is not a radical proposition; that is black-letter law.

For these reasons, we urge the court to identify tower dumps as *per se* general searches and prohibit law enforcement from employing this unconstitutional investigative technique.

I. Tower dumps are unconstitutional general searches because they are overbroad by their nature

Article I, Paragraph 7 of the New Jersey Constitution requires law enforcement to seek a warrant before obtaining an individual's cell-site location information (CSLI). *Earls*, 214 N.J. at 569.[2] On this front, New Jersey

[2] Although the State says it is not challenging the applicability of the warrant requirement to the tower dumps, it insinuates that the CSLI and call records in this case are somehow entitled to less protection because the people caught up in a tower dump use their cellphones "voluntarily." State's Reply at 3. But *Earls* explicitly rejects this distinction. *See Earls*, 214 N.J. at 584 ("[C]ell-

provides a "clear set of rules" to guide law enforcement: because every individual has a privacy interest in the "location of his or her cell phone," police require a warrant to obtain information about even just a single momentary datapoint of a cell phone's location, contrary to more equivocal out-of-state caselaw following the Fourth Amendment cited by the State. *Id.* at 588–89. *See, e.g., Hudson v. State*, 312 A.3d 615, 632 (Del. 2024) (suggesting with little analysis that a warrant is likely not required for all acquisition of CSLI).

But when applying the warrant requirement to tower dumps, which disclose a region's worth of peoples' CSLI all in one go, it is clear that a warrant should never be issued. By necessity, tower dumps are overbroad, not particular, and can never be justified by probable cause for the wide swath of people's CSLI and call records they capture. That renders the investigative technique an impermissible general search in all cases, and therefore *per se* unconstitutional. *See Feliciano*, 224 N.J. at 366.

---

phone users have no choice but to reveal certain information to their cellular provider. That is not voluntary disclosure in a typical sense; it can only be avoided at the price of not using a cell phone."). It is surprising that the State cites *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Miller*, 425 U.S. 435 (1976) for the proposition that information voluntarily shared with third parties is less private, considering that New Jersey has rejected the federal third-party doctrine embodied in *Smith*/*Miller* for nearly forty-five years. *See Earls*, 214 N.J. at 585.

To begin, tower-dump warrants are overbroad because they necessarily compel disclosure of the location information for hundreds or thousands of phone numbers, allowing police to track a myriad of individuals with no connection to the crime under investigation. For example, in one of the earliest known tower-dump cases, the FBI sought four tower dumps that reportedly returned the location information for *150,000 people*.[3] The tower-dump warrants in this case ultimately revealed the private information of over 10,000 people, all within just 90 minutes' worth of cellular tower data. Da016.[4]

Crucially, it would have been impossible in this case to narrow down the tower dump to capture fewer than several thousand people. The smallest unit of measurement that law enforcement can use when requesting a tower dump is a single cell tower. But in this case, a single AT&T cell tower serving the targeted residence yielded as many as 4,963 phone numbers. Da016.

Even tower dumps that could sweep in far fewer innocent people would still be irremediably overbroad. The government knows that most people swept up in a tower dump are uninvolved in any crime under investigation; they were simply in the same general region of the crime scene. Law enforcement can

---

[3] Ellen Nakashima, *Agencies Collected Data on Americans' Cellphone Use in Thousands of 'Tower Dumps'*, Wash. Post (Dec. 9, 2013), Aa24.

[4] "Da" = Defendant-Appellant's Appendix.

therefore never establish a sufficient nexus between hundreds or thousands of people's private data stored by cellular companies and the alleged offense. Just as Mr. Hunter argues, the logic that fuels tower dumps is the same logic behind "all-persons warrants," which are only valid when there is probable cause that all of the people in a location to be searched are involved in criminal activity. *See State v. De Simone*, 60 N.J. 319, 322 (1972) (requiring a "well-grounded suspicion" that links probable cause to particular subjects of the proposed search); *State v. Sims*, 75 N.J. 337, 350–51 (1978) (warrant authorizing search of service station was a general warrant, where there was no affirmation that known gamblers had been observed entering the building). But tower dumps may *never* meet this standard because there will never be probable cause that each of the hundreds or thousands of people connected to a particular cellular tower is involved in a specific crime.[5]

Nor are tower-dump warrants sufficiently particularized. Even if the State argues that the tower-dump warrants in this case specifically described

---

[5] *Accord Ybarra v. Illinois*, 444 U.S. 85, 86 (1979) ("[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."); *Berger v. New York*, 388 U.S. 41, 59 (1967) (decrying wiretapping of "conversations of any and all persons coming into the area covered by the [eavesdropping] device . . . without regard to their connection with the crime under investigation").

what authorities sought to search (cellular provider records), they could never specify the suspect under investigation. In this case, law enforcement did not even specify the particular cell towers for which they sought tower dumps on the face of the warrant. Instead, they applied for a warrant that left it entirely to the officers and the cellular providers to decide how many cell towers would be searched after the warrant had already been issued. Dca002[6] (failing to specify cell sites and leaving it to the executing agents' discretion to determine which cell sites would constitute "any other cell site location facing and in close proximity to" the crime scene); *see Marron v. United States*, 275 U.S. 192, 196 (1927) (holding that a proper search warrant should ensure "nothing is left to the discretion of the officer executing the warrant"); *State v. Muldowney*, 60 N.J. 594, 600 (1972) (disapproving of a warrant that "leaves the protection of the constitutional rights afforded the person to be searched to the whim of [the] officer").

This Court would not be the first to hold that tower dumps are unconstitutional general searches. Recently, a federal magistrate identified tower dumps as "categorically prohibited by the Fourth Amendment" for the same reasons as above:

---

[6] "Dca" = Defendant-Appellant's Confidential Appendix.

> [T]he Government is essentially asking the Court to allow it access to an entire haystack because it may contain a needle. But the Government lacks probable cause both as to the needle's identifying characteristics and as to the many other flakes of hay in the stack. . . . [T]he haystack here could involve the location data of thousands of cell phone users in various urban and suburban areas. . . . [T]he tower-dump warrant applications "present the exact sort of 'general, exploratory rummaging' that the Fourth Amendment was designed to prevent." And because they are "general warrants," they are "categorically prohibited by the Fourth Amendment."
>
> [*In re Four Applications for Search Warrants Seeking Information Associated with Particular Cellular Towers*, No. 3:25-CR-38-CWR-ASH, 2025 WL 603000, at *8 (S.D. Miss. Feb. 21, 2025), Aa47–48 (slip copy)].[7]

This makes sense. Just as no one would expect a court to authorize the search of every house on the block because one of the houses may belong to the perpetrator, neither can a warrant be issued to search the private cell phone records of thousands of people only because one of those people may have been the suspect. *See Marshall*, 199 N.J. at 616–17 (invalidating a warrant purporting to allow the search of a multi-unit building because police had not yet identified which unit belonged to the suspect). We urge the Court to draw the same conclusion and find tower dump warrants *per se* unconstitutional.

---

[7] Per N.J. Ct. R. 1:36-3, this unpublished opinion is provided because it is a recently-decided case that demonstrates a federal court's approach to similar factual circumstances and not because it constitutes binding precedent on this Court.

II. Tower dumps encourage the specific evils of a general search because they reveal private information that may be retained and utilized in future investigations without judicial oversight.

A. Tower dumps reveal personal details of an undoubtedly private nature, implicating our constitutional rights to privacy and freedom of association.

We normally do not invite the police to accompany us when we enter a doctor's office for a consultation, visit a political headquarters to plan a campaign, call a law firm to seek legal advice, or do anything else in our lives. However, at each moment our phones are our constant companions, compulsively reporting to our cellular provider our cell-site location information (CSLI) and records of when and to whom we talk. *See Carpenter v. United States*, 585 U.S. 296, 311 (2018) (citing *Riley*, 573 U.S. at 395); *see also Carpenter*, 585 U.S. at 313–14 ("Unlike the nosy neighbor who keeps an eye on comings and goings, [cellular providers] are ever alert, and their memory is nearly infallible.").

Tower dump records containing CSLI and call records reveal some of the most sensitive privacies of life for the hundreds to thousands of people caught up in their dragnet. Data on our movements throughout the day can betray information on families, our friends, our politics, our healthcare, our lifestyles, and much more. *See Earls*, 214 N.J. at 586 (citing *U.S. v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (cell-site location information "reflects a wealth of detail about [one's] familial, political, professional, religious, and

sexual associations")). The same goes for call records, which can reveal detailed facts about our lives through whom we call and text. *State v. Hunt*, 91 N.J. 338, 347 (1982) (citing *Smith*, 442 U.S. at 748 (Stewart, J., dissenting) (call histories "reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life")).

For these reasons, our Supreme Court has not hesitated in finding that the public has a strong reasonable expectation of privacy under Article I, Paragraph 7 in records of our cell-site location information and who we call. *Earls*, 214 N.J. at 569; *Hunt*, 91 N.J. at 348.[8] This makes out-of-state precedent like *Commonwealth v. Perry*, a Supreme Judicial Court of Massachusetts case analyzing the privacy interests implicated by tower dumps, less instructive for our purposes. 184 N.E.3d 745 (Mass. 2022). For example, although *Perry* decided that tower dumps were ultimately a Fourth Amendment search, *Perry* held that the fifty thousand uninvolved people whose data was captured in tower dumps were somehow "not subjected to a search in the constitutional sense" since the intrusion on the private lives of uninvolved

---

[8] Amici acknowledge that access to telephone billing records, while still requiring judicial oversight, does not require a warrant. *State v. Lunsford*, 226 N.J. 129, 155 (2016). Nonetheless, amici believe this case has no application to tower dumps because tower dump records are cell-site location information protected under *Earls*. Moreover, the combination of information is more revealing than either of CSLI or call records alone.

people was not as extensive as it was for the suspects being targeted. *Perry*, 184 N.E.3d at 768. In contrast, New Jersey follows the clearer and more privacy-respecting rule that *every single person* whose cellphone location is obtained by law enforcement, however momentarily, was subjected to an intrusion on their privacy. *Earls*, 214 N.J. at 588–89; *cf. State v. Johnson*, 193 N.J. 528, 543 (2008) (holding that the application of Art. I, Para.7 in individual cases should aim to "increase the privacy rights of all New Jersey's citizens and encourage law enforcement officials to honor fundamental constitutional principles").

Access to cell-site location information also raises significant First Amendment and Article I, Paragraph 6 freedom of association and speech. *See Application of Martin*, 90 N.J. 295, 325 (1982); *cf. Muldowney*, 60 N.J. at 600 (calling for careful consideration of search and seizure issues where First Amendment rights may also be at stake); *Stanford v. Texas*, 379 U.S. 476, 485 (1965) (searches must be conducted with "the most scrupulous exactitude" when the matter to be seized/searched implicates First Amendment freedoms). The constitutional right to freedom of association protects against state intrusion into the "choices to enter into and maintain certain intimate human relationships." *Roberts v. U.S. Jaycees*, 468 U.S. 609, 617 (1984). That right to maintain our own intimate relationships and political affiliations requires

privacy from improper government intrusion. *See NAACP v. Alabama*, 357 U.S. 449, 461 (1958) (recognizing "the vital relationship between freedom to associate and privacy in one's associations").

In short, privacy is essential to associational freedom, and associational freedom is essential to a free society. *See Buckley v. Valeo*, 424 U.S. 1, 25 (1976) (identifying freedom of association as "a right which, like free speech, lies at the foundation of a free society") (citation omitted). But the knowledge that the government may be watching cracks the foundations of that free society. *See Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms."). Tower dumps enable the police to learn not only who was near the scene of a crime, but also the identities of people who travel together, the attendees of a church or recovery group meeting, and other sensitive associations.[9]

Today, the potential chilling effect of government intrusion is made all-the-worse by law enforcement access to virtually effortless surveillance tools and techniques. *See id*. at 415–16 (noting the difficulty in keeping electronic

---

[9] The State claims that *Earls* does not stand for the proposition that cellular phone records are private or able to reveal your religious or political affiliations. State's Reply at 13. But that is explicitly the harm that *Earls* describes and protects against. *Earls*, 214 N.J. at 586.

surveillance in check given its low cost). New technologies reveal to law enforcement, with "breathtaking quality and quantity," a "highly detailed profile" of our "political, religious, amicable and amorous" associations, including the doctors we see, the attorneys we hire, the churches we visit, and much more. *People v. Weaver*, 909 N.E.2d 1195, 1199 (N.Y. 2009).

When law enforcement seizes thousands of cell-site location information and calling histories through a tower dump, they seize multiple neighborhoods' worth of rolodexes of private associations. The records readily allow investigators to infer "the identity of the individual with whom the user of a particular device was communicating at the moment the device connected to the cell site, and therefore provide investigators with significant insight into the individual's associations." *Perry*, 184 N.E.3d at 762. For example, tower dumps from the site of a large protest will not just capture who was present, but also can allow law enforcement to infer group membership, close ties between activists within the group, and more.[10] *See* Susan Landau & Patricia Vargas Leon, *Reversing Privacy Risks: Strict Limitations on the Use of Communications Metadata and Telemetry Information*, 21 Colo. Tech. L.J.

---

[10] For example, into 2014, the Ukrainian government reportedly used tower dumps to figure out who attended an anti-government protest. Andrea Peterson, *Ukraine's 1984 Moment: Government Using Cellphones to Track Protesters*, Wash. Post (Jan. 21, 2014), Aa28.

225, 286–87 (2023). This kind of intrusion into political affiliations and activities plainly infringes on First Amendment rights to political association and expression. *See Buckley*, 424 U.S. at 15.

B. Police can retain tower dump records indefinitely and use them as sources of general criminal intelligence, raising the specter of a general search.

The State insinuates that even if CSLI and call records are of a private nature, the search of those records via tower dumps is merely a one-time, incidental intrusion.[11] That is simply not true—even if a police officer never looks at or analyzes the call records of a particular uninvolved person in the course of a single investigation, nothing stops law enforcement from retaining the tower dump records and searching them in future cases regardless of any limitation in the original warrant. This extraordinary potential for "a general, exploratory rummaging" through tower dumps is precisely the evil of a general search that the Fourth Amendment and Article I, Paragraph 7 are aimed at preventing. *Coolidge*, 403 U.S. at 467.

Gratuitous tower dump records may have no utility in the immediate case, but it is not in law enforcement's interest to dispose of them when they

---

[11] *See, e.g.,* State's Reply at 3 (suggesting that the detailed cell-site records of "thousands of unrelated phone numbers" are less intrusive than being momentarily captured on surveillance camera).

might be used in future investigations. Police departments around the country already have practices of maintaining large databases of criminal intelligence information for their benefit, and there is a wide marketplace of tools available to analyze and derive private information from that data.[12] The tower dumps from one agency can also be retained, stockpiled, and shared across agencies to create an even more comprehensive view of activities in a region. *See, e.g.,* G.W. Schulz, *Virginia Police Have Been Secretively Stockpiling Private Phone Records*, Wired (Oct. 20, 2014), Aa17 (reporting an effort by five municipal police agencies in Virginia to "share telephone intelligence information derived from any source with the [task force] including: subpoenaed telephone call detail records, subpoenaed telephone subscriber information, and seized mobile devices").

Once a law enforcement agency sets up the infrastructure for storing and analyzing the data they have, that data analysis can be automatic and effortless. While amici are unaware of whether the Middlesex County Prosecutors Office

---

[12] These practices and tools reflect an approach criminal intelligence called "data fusion," whereby police data systems are designed to aggregate previously siloed and separate policing data, "such as call data records, social media posts, and financial transactions," map peoples' locations and social connections, and make that data available, searchable, and analyzable for future investigations. Inbar Goldstein, *From Raw Data to Informed Decisions: How Data Fusion Empowers Decision Intelligence*, Cognyte (July 2, 2023), Aa29.

employs specific tools or engages in any particular practice, the number of tools out there fills a clear demand from law enforcement for systems that can analyze the copious amounts of data they collect. For example, one vendor of cellular records analysis tools, CellHawk, markets its ability to "process a year's worth of cellphone records," including call detail records containing CSLI, "in 20 minutes." Sam Richards, *Powerful Mobile Phone Surveillance Tool Operates in Obscurity Across the Country*, The Intercept (Dec. 23, 2020), Aa4.[13]

Because cell-site location information call records can be aggregated across time to reveal a more complete picture of private life, it is irrelevant that a single tower dump request might appear to capture data from only a narrow window of time. Even a single snapshot of a community's call detail

---

[13] Cellebrite, a popular law enforcement vendor that sells cellphone analytics platforms to agencies in New Jersey, also offers an analysis program that "streamlines your investigative process, automates data ingestion, and uses advanced machine learning to analyze and visualize data from mobile, cloud, computer, [*call detail records*], and video sources." *Cellebrite Pathfinder*, Cellebrite (rev. Mar. 13, 2025), Aa36 (emphasis added). Another company called GraphAware boasts that its data analytics platform for law enforcement can give analysts a "unified view" of their criminal intelligence assets by extracting the links between people and map their whereabouts through their call detail records. *Accelerated Criminal Intelligence*, GraphAware (rev. Mar. 17, 2025), Aa32. Police analysts can use the platform to query records, automatically perform "co-offending network analysis," or use artificial intelligence to generate "risk scores" and other insights from the data beyond any single investigation.

records through a tower dump can be combined with others to construct a broader picture of activity. *See, e.g., Perry*, 184 N.E.3d at 763 (noting that multiple, smaller snapshots from tower dumps on different days can be more revealing than a single, larger snapshot from one day); *U.S. v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010) ("Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month."); Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 Sup. Ct. Rev. 205, 205 (2015) (noting that "the government can learn more from a given slice of information if it can put that information in the context of a broader pattern, a mosaic").

Ultimately, any use of the fruits of a tower dump past the end of an investigation will violate the warrant that purportedly authorized the tower dump in the first instance. This risk is not hypothetical or attenuated from the original search, but rather is a natural outgrowth of law enforcement's use of tower dumps. For this reason, this Court should find that tower dumps enable general searches and find them *per se* unconstitutional.

III. The tower dumps in this case were overbroad, gratuitous, and enable the sort of data retention that can make tower dump searches dangerous.

The tower dumps requested in the instant case were an unconstitutional general search. In particular, there were three deficiencies in the State's warrant application that rendered the tower dumps especially overbroad, and which demonstrate how tower dumps run afoul of our constitutional privacy safeguards.

a. The State made no attempt to narrow their tower dump request.

Although we urge the Court to recognize that a tower dump can *never* be sufficiently narrowed, the State failed to even try. The State's warrant requests tower dumps from "the cell site(s) providing service to the location(s) listed below and any other cell site location facing and in close proximity to 1521 Park Avenue, South Plainfield, NJ 07080[.]" Dca003. As Mr. Hunter's expert explains, a "network survey" of the area by law enforcement could have allowed them to identify the main "Serving" cell site and "the top two or three Neighboring towers/antennas," and subsequently only request tower dumps from those cell towers. Dca016. This would have at least narrowed the requests to Verizon, which returned eight towers' worth of data, and T-Mobile, which returned ten towers' worth of data.[14] Da011; Da014. Instead, the warrant left it

[14] Though, as noted in Point I, AT&T and Sprint's returns still included thousands of phone numbers despite only covering one tower's and three tower's worth of data respectively. Da007; Da016. Thus, in this case, even a

up to the broad discretion of the officers and the cellular companies to decide how much data they would report back. The fact that it has pinpointed the locations of thousands of innocent people demonstrates the overbreadth of this warrant.

Further, the State's warrant sought a laundry list of information above and beyond what is ordinarily in a tower dump. The warrant includes not only "cell site information for the period requested," but also the "account number, account type, subscriber account name, billing address, subscriber's social security number, [and] subscriber's date of birth" for every single cellular subscriber caught in the dragnet. Dca003. Even if the cellular providers did not apparently provide this extra information, the request is overbroad and excessive on its face. The State could have easily narrowed its request to only the categories of information that were strictly necessary to the investigation. Once it identified suspects, only then should it have sought identifying data.

b. Law enforcement should have known that the tower dumps were unnecessary to advance this investigation from its outset.

In this case, law enforcement sought tower dumps only nine days into their investigation. At that point, the State already had several targeted leads it

---

request for fewer cell towers would likely have failed to narrow the request sufficiently.

should have pursued and ruled out before resorting to tower dumps. Dca005; Dca007 (warrant application describing leads that did not require phone records to pursue). If tower dumps can be so easily requested in cases where they are patently unnecessary, that enhances the risk of improper data retention and future misuse. *See supra* Point II.C.[15]

It is also dangerous to authorize tower dumps when there are no limiting principles for the analysis of the tower dump data; here, law enforcement obtained the tower dumps because they knew the suspect had made "several phone calls" while committing the crime. These facts alone do not allow investigators to distinguish the suspect from all of the other people caught up in the tower dump records, many of whom likely placed multiple calls themselves.

For that reason, tower dump warrants are often only useful and necessary—and more protective of third-party privacy—when police suspect that a single offender was responsible for different crimes at different times

---

[15] Curiously, the State also says that it "knew exactly who they were looking for, when, and simply needed verification." *See* State's Opp. to Mot. for Leave to Appeal at 2 (filed Jan. 13, 2025). If that is the case, why did the State not seek only ordinary, targeted cell-site location information of the kind authorized under *Earls*? There clearly was no law-enforcement need to sweep up the data of ten thousand people in-and-around South Plainfield through tower dumps, making the resulting intrusion even more gratuitous.

and places. In those cases, investigators can easily rule out uninvolved people by comparing the tower dumps with each other to discover who, if anyone, may have been present at multiple crime scenes. In *Perry*, for example, police were investigating a string of robberies they had probable cause to believe were committed by the same person; the Supreme Judicial Court of Massachusetts found that because the police could limit their use of tower dumps to "isolate potential suspects by determining which, if any, individuals had been near the scene of two or more offenses," the privacy of people for whom there was no probable cause would be preserved. *Perry*, 184 N.E.3d at 66.[16] No such limitation was possible in this case, which is why the warrant that was authorized was a general warrant.

c. The warrant did not obligate the State to follow a protocol for the proper acquisition, use, retention, and disposal of tower dump records.

Finally, the warrants imposed no obligation on the State to follow any data retention or disposal rules to limit to the fullest extent possible invasions

[16] Although it may appear counterintuitive to say that multiple-crime tower dumps can be more privacy-preserving, since they may sweep up more people initially, searches involving multiple crime scenes will ultimately produce datasets that are smaller in size, more particularized, and more closely tied to probable cause. That is because the analysis in those cases should be limited to only those people present in multiple tower dumps. All other uninvolved people can be easily ruled out and discarded from the data.

into the privacy of people lacking any role in the criminal offense under investigation.[17] A warrant could, for example, require a "filter team" segregated from the primary investigators to perform the tower dump analysis and only return those results relevant to the current investigation.[18] A warrant should also explicitly require the prompt deletion of uninvolved peoples' information, except as necessary to satisfy *Brady* and other defense disclosure obligations.[19] Without these sorts of limitations, which other courts have had no trouble instituting, the resulting warrants have the character of general warrants.

---

[17] *See In re Application of the U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012) (imposing this requirement); *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, and Verizon Wireless to Disclose Cell Tower Log Information*, 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014) (same).

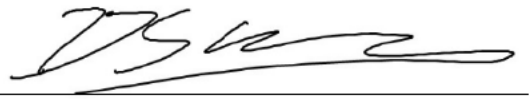
[18] *See, e.g., U.S. v. Comprehensive Drug Testing, Inc*., 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, C.J., concurring) ("Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party.").

[19] *Cf. In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *4 (N.D. Ill. Nov. 9, 2015), Aa52 (in granting warrant to use cell site simulator to locate suspect's phone, requiring that "law enforcement officers must immediately destroy all data other than the data identifying the cell phone used by the target").

CONCLUSION

Without any limitation on their breadth, the warrants issued in this case were exactly the sort of "general warrants" that our constitutional order forbids. For the above reasons, the Court should hold that the unprecedented, indiscriminate, and dragnet nature of tower dumps means they are unconstitutional general searches and prohibit their use as a law enforcement investigative technique.

Respectfully submitted,



Dillon Reisman (374142021)
Ezra D. Rosenberg (012671974)
Jeanne LoCicero (024052000)
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY FOUNDATION
[redacted]
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
dreisman@aclu-nj.org
erosenberg@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
[redacted]
Tel: (415) 343-0758
jgranick@aclu.org

* *Pro hac vice* pending
Attorneys for Amici Curiae

Dated: April 10, 2025