# SUPREME COURT OF NEW JERSEY DOCKET NO. A-53-11 (068765)

STATE OF NEW JERSEY,

Plaintiff-Respondent,

v.

THOMAS W. EARLS,

Defendant-Appellant.

#### CRIMINAL ACTION

On Appeal From a Final Order of the Superior Court, Appellate Division, Affirming the Judgment of Conviction.

### Sat Below:

Hon. Anthony J. Parrillo, P.J.A.D. Hon. Stephen Skillman, J.A.D. Hon. Patricia B. Roe, J.A.D.

# SUPPLEMENTAL BRIEF OF AMICI CURIAE, THE AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY FOUNDATION AND THE ASSOCIATION OF CRIMINAL DEFENSE LAWYERS OF NEW JERSEY

Rubin M. Sinins, Esq.
Javerbaum Wurgaft Hicks
Kahn Wikstrom & Sinins, P.C.
201 Washington Street
Newark, NJ 07102
(973) 642-7005
rsinins@lawjw.com
Attorneys for
ACLU-NJ and ACDL-NJ

On the Brief: Rubin M. Sinins, Esq. Alexander Shalom, Esq. Alexander Shalom, Esq.
Edward Barocas, Esq.
Jeanne LoCicero, Esq.
American Civil Liberties
Union of New Jersey Foundation
P.O. Box 32159
Newark, NJ 07102
(973) 854-1714
ashalom@aclu-nj.org
Attorneys for the ACLU-NJ

Jeffrey S. Mandel, Esq. PinilisHalpern, LLP 160 Morris Street Morristown, NJ 07960 (973) 401-1111 jmandel@pinilishalpern.com Attorneys for ACDL-NJ

## TABLE OF CONTENTS

TABLE OF AUTHORITIESii
PRELIMINARY STATEMENT
ARGUMENT2
I. NEITHER RECOGNIZING AN EXPECTATION OF PRIVACY NOR IMPOSING A WARRANT REQUIREMENT TO OBTAIN CELL PHONE LOCATION DATA CONSTITUTES A NEW RULE OF LAW2
A. Expectation of Privacy4
B. Warrant Requirement6
II. ASSUMING THAT THE WARRANT REQUIREMENT ANNOUNCES A NEW RULE OF LAW, IT IS A CLOSE QUESTION WHETHER IT IS ENTITLED TO RETROACTIVE APPLICATION IN CIRCUMSTANCES WHERE LAW ENFORCEMENT COMPLIED WITH THE REQUIREMENTS OF THE WIRETAP ACT
A. Purpose of the Rule10
B. Reliance
C. Administration of Justice
III. CELL PHONE USERS HAVE A REASONABLE EXPECTATION OF PRIVACY IN THE LOCATION OF MODERN CELL PHONES NOT ONLY UNDER THE NEW JERSEY CONSTITUTION BUT, LIKELY, ALSO UNDER THE UNITED STATES CONSTITUTION
IV. THE CURRENT STATE OF TECHNOLOGY RELATING TO CELL PHONE LOCATION TRACKING ENABLES PINPOINT TRACKING ON A CONTINUOUS BASIS
CONCLUSION 1.0

#### TABLE OF AUTHORITIES

#### Cases

<u>Arizona v. Hicks</u> , 480 <u>U.S.</u> 321 (1987)
<u>Cardwell v. Lewis</u> , 417 <u>U.S.</u> 583 (1974) 5 n.2
<u>Florida v. Riley</u> , 488 <u>U.S.</u> 445 (1989)
<u>Guest v. Leis</u> , 255 <u>F.3d</u> 325 (6th Cir. 2001)
In re Application of the United States for an Order  Authorizing the Release of Historical Cell-Site  Information, 809 F.Supp. 2d 113 (E.D.N.Y. 2011)
In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304 (3d Cir. 2011)
In re Application of the United States of America for Historical Cell Site Data, 747 F.Supp. 2d 827 (S.D. Texas 2010)
<u>Katz v. United States</u> , 389 <u>U.S.</u> 347 (1967)
<u>Kyllo v. United States</u> , 533 <u>U.S.</u> 27 (2001)8-9
<u>Schneckloth v. Bustamonte</u> , 412 <u>U.S.</u> 218 (1973)
<u>Smith v. Maryland</u> , 442 <u>U.S.</u> 735 (1979)
<u>State v. Alston</u> , 88 <u>N.J.</u> 211 (1981)
<u>State v. Carty</u> , 332 <u>N.J. Super.</u> 200 (App. Div. 2000)11
<u>State v. Carty</u> , 170 <u>N.J.</u> 632 (2002)
<u>State v. Carty</u> , 174 <u>N.J.</u> 351 (2002)
<u>State v. Cassidy</u> , 179 <u>N.J.</u> 150 (2004)
<u>State v. Cummings</u> , 184 <u>N.J.</u> 84 (2005)
<u>State v. Cupe</u> , 289 <u>N.J. Super.</u> 1 (App. Div.), <u>certif.</u> denied, 144 N.J. 589 (1996)

<u>State v. Davila</u> , 203 <u>N.J.</u> 97 (2010)
<u>State v. Dock</u> , 205 <u>N.J.</u> 237 (2011)
<u>State v. Domicz</u> , 188 <u>N.J.</u> 285 (2006)
<u>State v. Hempele</u> , 120 <u>N.J.</u> 182 (1990)
<u>State v. Henderson</u> , 208 <u>N.J.</u> 208 (2011)
<u>State v. Hodge</u> , 426 <u>N.J. Super.</u> 321 (App. Div. 2012)15
<u>State v. Hunt</u> , 91 <u>N.J.</u> 338 (1982)
<u>State v. Johnson</u> , 68 <u>N.J.</u> 349 (1975)
<u>State v. Knight</u> , 145 <u>N.J.</u> 233 (1996)
<u>State v. Laboo</u> , 396 <u>N.J. Super.</u> 97 (App. Div. 2007) 14 n.10
<u>State v. McAllister</u> , 184 <u>N.J.</u> 17 (2005)
<u>State v. Mangold</u> , 82 <u>N.J.</u> 575 (1980) 5 n.2
<u>State v. Mollica</u> , 114 <u>N.J.</u> 329 (1989)
<u>State v. Pena-Flores</u> , 198 <u>N.J.</u> 6 (2009) 5 n.2
State v. Pompa, 414 N.J. Super. 219 (App. Div. 2010) 5 n.2
<u>State v. Purnell</u> , 161 <u>N.J.</u> 44 (1999)
<u>State v. Reid</u> , 194 <u>N.J.</u> 386 (2008)
State v. Yanovsky, 340 N.J. Super. 1 (App. Div. 2001) 10-11
<u>United States v. Block</u> , 590 <u>F.</u> 2d 535 (4th Cir.1978)
<u>United States v. Jacobsen</u> , 466 <u>U.S.</u> 109 (1984)
<u>United States v. Jones</u> , 132 <u>S.Ct.</u> 945 (2012)7-8
<u>United States v. Karo</u> , 468 <u>U.S.</u> 705 (1984)7-8
United States v. Miller, 425 U.S. 435 (1976)

<u>United States v. Nilsen</u> , 482 <u>F. Supp.</u> 1335 (D.N.J. 1980)
<u>United States v. Warshak</u> , 631 <u>F.</u> 3d 266 (6 <sup>th</sup> Cir. 2010)3
Constitutions, Statutes and Rules
N.J. Const. art. I, $\P$ 7
<u>N.J.S.A.</u> 2A:156A-29a9
<u>N.J.S.A.</u> 2A:156A-29c
<u>N.J.S.A.</u> 47:1A-1 et seq
2009 NJ Sess. Law Serv. Ch. 184 (SENATE 2841) (WEST) 14 n. 10
Other Authorities
http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_berkeleytwnshppd_berkeleytwnshpnj.pdf 12 n.8
http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_camdenpd_camdennj.pdf
http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_elizabethpd_elizabethnj.pdf
http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_eveshamtwnshppd_eveshamtwnshpnj.pdf 12 n.5
http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_hamiltonpd_hamiltonnj.pdf
http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_hobokenpd_hobokennj.pdf
http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_lakewoodpd_lakewoodnj.pdf
http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_mountlaureltwnshppd_mountlaureltwnshppi.pdf
http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_newarkpd_newarknj.pdf

http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_northbrunswickpd_northbrunswicknj.pdf13-14 n.9
http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-documents-
new-jersey12

#### PRELIMINARY STATEMENT

Amici contend that, were this Court to hold that citizens maintain an expectation of privacy in cell phone location data and that a warrant is required to obtain that data, it would not announce a new rule of law. Given the nature of cell phone location information and this Court's precedent pertaining to information of this kind, there can be no reasonable debate that currently existing law protects citizens' expectations of privacy in cell phone location information, mandating at least some judicial oversight. See Point I.A. (infra at 4-6). While requiring a warrant to obtain such information (as opposed to requiring merely some form of process) would be plausibly novel, even the warrant requirement merely represents a logical extension of existing law. See Point I.B. (infra at 6-9).

Cell phone location data can be obtained in four ways: 1) by request; 2) by subpoena; 3) by court order; or 4) by warrant. Law enforcement violates well-established constitutional norms when it obtains this data without at least minimal process. Whenever a citizen has an expectation of privacy in certain information or documents, police may not simply seize the protected material at will without running afoul of the Constitution. While there are some circumstances where a lawfully issued subpoena is sufficient to protect citizens' privacy interests, New Jersey's Wiretap Act

mandates additional judicial oversight. All law enforcement is therefore now on notice that obtaining cell phone location information merely through request or a subpoena violates the law. This statutory requirement codifies citizens' expectation that location information will not be released to law enforcement without judicial approval. As such, for those categories of cases, retroactivity analysis is unnecessary (or, if conducted, clearly counsels in favor of full retroactivity).

If the Court determines that the specific warrant requirement represents a new rule of law, <u>amici</u> concede that retroactivity analysis regarding that requirement is a closer question. <u>See</u> Point II (infra at 9-16).

#### **ARGUMENT**

#### POINT I

NEITHER RECOGNIZING AN EXPECTATION OF PRIVACY NOR IMPOSING A WARRANT REQUIREMENT TO OBTAIN CELL PHONE LOCATION DATA CONSTITUTES A NEW RULE OF LAW.

This Court has established that a "new rule of law" is announced when a decision "breaks new ground or establishes a new obligation on the State[]...[or] if the result was not dictated by precedent at the time of defendant's conviction." State v. Knight, 145 N.J. 233, 250-51 (1996); State v. Cummings, 184 N.J. 84, 97 (2005). In other words, "a decision involving an 'accepted legal principle' announces a new rule," where the decision's "application of that general principle is 'sufficiently novel and unanticipated.'" Id.

at 251; <u>Cummings</u>, 184 <u>N.J.</u> at 97; <u>State v. Dock</u>, 205 <u>N.J.</u> 237, 255 (2011). This has been described as a decision's "sudden and generally unanticipated repudiation of a long-standing practice." <u>State v. Purnell</u>, 161 <u>N.J.</u> 44, 53 (1999) (quoting <u>State v. Cupe</u>, 289 <u>N.J. Super.</u> 1, 12 (App. Div.), <u>certif. denied</u>, 144 <u>N.J.</u> 589 (1996)).

This Court's long-standing constitutional jurisprudence both recognizes privacy interests in data such as that at issue here, (see, e.g., State v. Reid, 194 N.J. 386 (2008)), and mandates a warrant for the acquisition of similar, content-based information. generally, United States v. Jacobsen, 466 U.S. 109, 114 (1984) (warrant required to read letters); United States v. Warshak, 631 F.3d 266, 285-88 (6<sup>th</sup> Cir. 2010) (warrant required to read emails). Further, in New Jersey, there is also an independent statutory basis for requiring judicial intervention before allowing law enforcement to obtain cell phone location data. N.J.S.A. 2A:156A-29c. Thus, neither a general requirement of judicial process attending a search for cell phone location information, nor a specific warrant requirement, departs from existing law. Rather, those requirements are "dictated by precedent." Knight, 145 N.J. at 250-51; Cummings, 184 N.J. at 97. They neither "break new ground" nor establish "a new obligation upon the State." Id.

That even the warrant requirement is an anticipated principle is reflected by the State's concession that warrants are generally

already sought for cell phone location data. (Psb3)<sup>1</sup>.

#### A. Expectation of Privacy

Applying this Court's precedent on Article I, paragraph 7 of the New Jersey Constitution, there is undoubtedly an expectation of privacy in one's cell phone location data, requiring at least some form of court process. For full discussion, see amici's main brief at pages 15 through 36.

This Court has recognized that citizens do not expect law enforcement to have unimpeded access to private information that is "integrally connected to [their] essential activities of today's society." Reid, 194 N.J. at 398. This rule of law has been applied to toll call billing records, State v. Hunt, 91 N.J. 338 (1982), bank records, State v. McAllister, 184 N.J. 17, 26 (2005), utility records, State v. Domicz, 188 N.J. 285, 299 (2006), and Internet Service Provider records, Reid, 194 N.J. at 389. All these records share the same fundamental nature of being information that is essential to modern life and which, if disclosed to law enforcement, can tell a great deal about our lives. Reid, 194 N.J. at 398.

Cell phone data information shares that same fundamental nature. Cell phone location - because it exposes one's whereabouts and, potentially, one's associations - divulges perhaps even more personal information. There exists no principled reason to find a

<sup>&</sup>lt;sup>1</sup> Psb refers to the State's First Supplemental Brief, dated July 11, 2012; Abr refers to <a href="mailto:amici">amici</a>'s Brief, dated February 27, 2012.

lesser expectation of privacy in cell phone location data.

Further, once a particular category of information is deemed protected, the Court need not specifically enumerate every piece of information that might fall within that category for the protection to apply thereto. <sup>2</sup> Thus, as with prior such cases, for law enforcement to obtain information of this sensitive nature, judicial process is required.

Unlike federal courts, this Court has found a legitimate expectation of privacy in several types of data, regardless of the fact that it may be held by third parties. Compare Hunt, 91 N.J. at 343 (expectation of privacy in phone-toll billing records) and State v. Mollica, 114 N.J. 329, 335 (1989) (expectation of privacy in hotel phone records) with Smith v. Maryland, 442 U.S. 735, 746 (1979) (no expectation of privacy in phone-toll billing records); compare McAllister, 184 N.J. at 26 (expectation of privacy in bank records) with United States v. Miller, 425 U.S. 435, 442 (1976) (no expectation of privacy in bank records); compare Domicz, 188 N.J. at 299 (acknowledging possible expectation of privacy in utility records) with Jacobsen, 466 U.S. at 117 (no expectation of privacy

To illustrate, once courts recognized an expectation of privacy in motor vehicles, see, e.g. Cardwell v. Lewis, 417 U.S. 583, 589 (1974), it was unnecessary to explicitly find such an expectation for specific types of vehicles. See, e.g. State v. Mangold, 82 N.J. 575, 587 (1980) (expectation of privacy in contents of a van); State v. Pena-Flores 198 N.J. 6, 12 (2009) (expectation of privacy in Ford Expedition, a Sports Utility Vehicle); State v. Pompa, 414 N.J. Super. 219, 233 (App. Div. 2010) (expectation of privacy in sleeper cabin of tractor trailer).

where information is revealed to a third-party); <a href="compare Reid">compare Reid</a>, 194</a>
<a href="N.J.">N.J.</a> at 389 (expectation of privacy in Internet Service Provider records) <a href="with">with</a>, <a href="e.g.">e.g.</a>, <a href="Guest v. Leis">Guest v. Leis</a>, <a href="255">255</a> <a href="F.3d">F.3d</a> <a href="325">325</a>, <a href="336">336</a> (6th Cir. 2001)</a> (no expectation of privacy in Internet Service Provider records).

Therefore, rather than representing a break from prior precedent, affirming the necessity of judicial oversight for law enforcement to obtain private information of this nature is merely a logical application of this Court's consistent commitment to protecting New Jerseyans' sensitive information from unreasonable searches and seizures in the modern world.

#### B. Warrant Requirement

Previously-established law goes even further than recognition of an expectation of privacy in sensitive information such as is present here. Our State and Federal Constitutions require a warrant for the seizure of content-based information in a sphere of privacy.

Katz v. United States, 389 U.S. 347, 356 (1967). Warrants have been long-required for searches and seizures in innumerable contexts.

See, e.g., United States v. Nilsen, 482 F. Supp. 1335, 1337 (D.N.J. 1980) (discussing search warrants of a home, an automobile, and a post office box). These situations include various types of electronic monitoring. See, e.g., United States v. Jones, 132 S. Ct. 945, 949 (2012) (GPS attached to car); United States v. Karo, 468 U.S. 705, 716 (1984) (beeper surveillance).

That the police have been obligated to seek judicial approval

before engaging in such surveillance reflects the long historical foundation of the warrant requirement. Requiring a warrant for cell phone location data breaks no new legal ground. Warrants have previously been required for searches involving thermal imaging (Kyllo v. United States, 533 U.S. 27, 40 (2001)) and other electronic surveillance devices. Jones, 132 S. Ct. at 949; Karo, 468 U.S. at 716. Personal data, derived from suitcases (See United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978) (stating that the law's "enclosed spaces," including suitcases, are frequently objects of one's highest privacy expectations)) and garbage contents (State v. Hempele, 120 N.J. 182, 198 (1990)), have long required warrants for their acquisition.

The warrant requirement for cell phone data is a logical continuation of precedent. It is not a repudiation of long-standing practice. Warrants are required to search homes, closed containers and other areas where law enforcement cannot see. See, e.g., State v. Cassidy, 179 N.J. 150, 159-60 (2004) (home); Block, 590 F.2d at 541 (suitcases); Arizona v. Hicks, 480 U.S. 321, 324-35 (1987) (backside of stereo equipment). Warrants are further required when surveillance is performed by electronic visual enhancement, with or without the assistance of cell phone providers. See, e.g., Kyllo, 533 U.S. at 40; Florida v. Riley, 488 U.S. 445, 455 (1989) (O'Connor, J., concurring) (explaining that expectation of privacy, and warrant requirement, turn on whether law enforcement is utilizing technology

commonly available to the public). Cell phone location data is merely another type of personal information that law enforcement seeks to seize through electronic enhancement. The warrant requirement imposes no new obligation upon the State.

The reason why warrants were not required for ISP and billing records was because those records, in themselves, arguably disclose no content-based information. However, that is not the case here. Cell phone location records require greater protection than those records. Location data is inherently content-based and discloses more private information about an individual. As discussed in depth in <a href="mailto:amici">amici</a>'s main brief at pages 15 through 36, disclosure here is more akin to the searches at issue in Kyllo.

As discussed at greater length below (<u>infra</u> Point II.B), the warrant requirement is likewise anticipated by the State. The State acknowledges here that police generally obtain warrants to acquire cell phone location data. (Psb3). Moreover, the seizure of data from cell phones – be it the contents of calls, the contents of email, or other records stored on the phone itself – already requires a warrant. N.J.S.A. 2A:156A-29a. So the warrant requirement for cell phone location data may hardly be considered unanticipated and is simply an appropriate pronouncement based on precedent.

In short, neither the finding of an expectation of privacy nor a warrant requirement would announce a new rule of law. Retroactive analysis is, accordingly, unnecessary.

#### POINT II

ASSUMING THAT THE WARRANT REQUIREMENT ANNOUNCES A NEW RULE OF LAW, IT IS A CLOSE QUESTION WHETHER IT IS ENTITLED TO RETROACTIVE APPLICATION IN CIRCUMSTANCES WHERE LAW ENFORCEMENT COMPLIED WITH THE REQUIREMENTS OF THE WIRETAP ACT.

As noted above, <u>amici</u> contend that this Court would not create a new rule of law, either by recognizing a legitimate expectation of privacy in cell phone location information or by requiring law enforcement to specifically seek a warrant. However, assuming the Court holds otherwise regarding the warrant requirement, <u>amici</u> recognize that, in cases where police relied on the procedures set forth in the Wiretap Act (N.J.S.A. 2A:156A-29c) - which allows for the seizure of location information not only based on a warrant, consent, or exigency, but also based on a court order on less than probable cause - the question of retroactivity is less clear.

It is well-established that:

[i]f a decision indeed sets forth a "new rule," three factors generally are considered to determine whether the rule is to be applied retroactively: '(1) the purpose of the rule and whether it would be furthered by a retroactive application, (2) the degree of reliance placed on the old rule by those who administered it, and (3) the effect a retroactive application would have on the administration of justice.'

[Knight, 145 N.J. at 251 (internal citations omitted).]

There is no doubt that, assuming that the mere finding of an expectation of privacy in cell phone location information was deemed

a new rule of law, retroactivity analysis would easily favor full retroactivity. The purpose of the rule would be furthered by ensuring that prior breaches of privacy would be remedied, all law enforcement officials should have been on notice through constitutional, and more recently statutory, law, that some form of process was required, and the number of cases to which the "new" rule would apply (cases where information was obtained with no process) would be minimal.

The warrant requirement, however, would require a more detailed analysis. As discussed below, while the purpose of the rule would be furthered by retroactive application, there may have been reliance on the "old" rule by law enforcement who abided by societal norms as codified by the procedures set forth in the Wiretap Act, N.J.S.A. 2A:156A-29c. Nevertheless, the State concedes that warrants are usually obtained, so retroactive application is unlikely to have a great impact on the administration of justice.

#### A. Purpose of the Rule

In considering the first question, it is useful to examine the ways in which New Jersey courts have conducted retroactivity analysis in other search and seizure contexts. It is true that "when the new rule is an exclusionary rule, the purpose of which is solely to deter illegal police conduct, it is virtually never given retroactive effect." State v. Yanovsky, 340 N.J. Super. 1, 9 (App. Div. 2001). That said, "where exclusion of evidence obtained in violation of a

defendant's rights is not the sole purpose of the new rule," id., evaluation of the other factors is required. In Yanovsky, which analyzed the retroactivity of State v. Carty, 332 N.J. Super. 200 (App. Div. 2000)<sup>3</sup>, the Appellate Division recounted the rationales behind Carty's holding. In addition to the ordinary purpose to "exclude the State's use of ill-gotten evidence," Yanovsky, 340 N.J. Super. at 10, the holding's "purpose also include[d]: (1) protection of travelers from unwarranted harassment, embarrassment and inconvenience resulting from baseless requests for consent to search, even where no evidence of crime is found, and (2) attribution of the force of law to the pre-existing policies of the state police." Id.

Similar rationales would animate this Court's finding of a warrant requirement in cell phone location data. In addition to deterring law enforcement from using the fruits of an illegal search, a warrant requirement would ensure that citizens' private location information — obtained prior to the announcement of a warrant requirement — is not stored, maintained, or utilized by law enforcement, unless they have relied on judicial process. Otherwise, what, for example, would preclude the State — upon receipt of this Court's request for supplemental briefing — from obtaining through the use of a subpoena, volumes of cell phone location

 $<sup>^3</sup>$  This Court eventually directly addressed the retroactive application of Carty. State v. Carty, 170 N.J. 632, 651 (2002), modified by 174 N.J. 351 (2002).

information for use in future investigations? Given the vast amount of private information contained in cell phone location data, citizens must be assured that it will only be collected, stored, and used in circumscribed situations. The privacy and associational interests implicated by unimpeded government access to cell phone location data were discussed in amici's main brief. Abr 28-40.

Accepting that there is a non-deterrent basis for the requirement, the Court must examine the reliance and administration of justice factors.

#### B. Reliance

As noted, the State concedes that when this data is needed, warrants are generally sought. (Psb 3). But, there is even more evidence that the State only rarely fails to obtain a warrant for this data where the situation is not emergent and the subscriber has not provided consent. In August of 2011, the American Civil Liberties Union of New Jersey, as part of a coordinated nationwide effort, sent requests under the Open Public Records Act, N.J.S.A. 47:1A-1 et seq., to New Jersey's fifty largest police departments. The ACLU-NJ explained that, because of growing concern over cell phone tracking, it sought records on policies, procedures, and use of cell phone location tracking. (Available at: http://www.aclu.org/protecting-civil-liberties-digital-age/cellphone-location-tracking-documents-new-jersey). While departments did not provide responses useful to the inquiry into reliance, some did. For example, Camden suggested that it only proceeded when it had obtained a warrant<sup>4</sup> and Evesham,<sup>5</sup> Lakewood,<sup>6</sup> and Mount Laurel,<sup>7</sup> among many others, suggested they procured Communications Data Warrants unless the exigencies of the situation precluded doing so.

The OPRA responses made reference to all four methods authorized under the Wiretap Act (warrant, consent, exigency, and court order). Some departments, however, made troubling references to obtaining cell phone location information without utilizing any judicial process. In other words, some departments may be obtaining cell

http://www.aclu.org/files/cellphonetracking/20120328/ celltrackingpra\_camdenpd\_camdennj.pdf

http://www.aclu.org/files/cellphonetracking/20120328/ celltrackingpra eveshamtwnshppd eveshamtwnshpnj.pdf

http://www.aclu.org/files/cellphonetracking/20120328/ celltrackingpra\_lakewoodpd\_lakewoodnj.pdf

<sup>&</sup>lt;sup>7</sup> http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra mountlaureltwnshppd mountlaureltwnshpnj.pdf

<sup>8</sup> See, e.g., for warrants, Newark:
http://www.aclu.org/files/cellphonetracking/20120328/
celltrackingpra\_newarkpd\_newarknj.pdf;
for consent, Elizabeth:
http://www.aclu.org/files/cellphonetracking/20120328/
celltrackingpra\_elizabethpd\_elizabethnj.pdf;
for exigency, Hamilton:
http://www.aclu.org/files/cellphonetracking/20120328/
celltrackingpra\_hamiltonpd\_hamiltonnj.pdf;
for judicial orders, Berkeley Township,
http://www.aclu.org/files/cellphonetracking/20120328/
celltrackingpra\_berkeleytwnshppd\_berkeleytwnshpnj.pdf

<sup>9</sup> See, e.g., for reference to a "subpoena," Hoboken:

phone location data in violation of clearly established statutory, if not constitutional, law.

To the extent that law enforcement either used a subpoena or, as happened in this case, no process whatsoever, it cannot claim to have relied on an old rule of law. 10 However, while the number of cases where a court order (but not a warrant) was used might not be great, those departments can plausibly argue that they relied on then-existent societal norms (as expressed in statutory law). Thus, if this Court finds that the warrant requirement is a new rule of constitutional law that was not dictated by the Court's existing jurisprudence, departments that relied on court orders would have had no reason to believe that their actions were improper.

http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra\_hobokenpd\_hobokennj.pdf; for reference to obtaining prosecutorial approval, North Brunswick: http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra northbrunswickpd northbrunswicknj.pdf

Amici acknowledge that the Wiretap Act was amended to explicitly include limitations on the acquisition of cell phone location data effective January 12, 2010 (2009 NJ Sess. Law Serv. Ch. 184 (SENATE 2841) (WEST)). Therefore, if, prior to that date, law enforcement acquired such data through the use of a valid subpoena, it could arguably contend that there existed no statutory prohibition. Still, for all the reasons discussed in Point I, supra, amici maintain that constitutional norms dictated that a subpoena was insufficient to justify such a search. Further, it is worth noting that, prior to the amendment of the Wiretap Act, law enforcement often sought Communications Data Warrants to obtain cell phone location information. See, e.g., State v. Davila, 203 N.J. 97, 103-04 (2010) (noting use, in 2003, of Communications Data Warrant to track stolen cellphone); State v. Laboo, 396 N.J. Super. 97, 99 (App. Div. 2007) (same in 2005).

#### C. Administration of Justice

In analyzing the effect that retroactive application of a new rule would have on the administration of justice:

[c]ourts should look to data produced to determine the extent to which, if any, the administration of justice will be impacted. The longer the prior rule has been in effect, however, the less likely there will be a need for such data because significant impact upon the administration of justice may be presumed.

[State v. Hodge, 426 N.J. Super. 321, 335 (App. Div. 2012) (citing State v. Henderson, 208 N.J. 208, 302 (2011)).]

Pursuant to this Court's Order requiring supplemental briefing — the State must produce data to determine the extent to which the administration of justice would be impacted by a warrant requirement. Based on the information described in Section I.B. above, <a href="mailto:amicion">amicion</a> believe the numbers of prior actions that will be effected will be minimal.

The submission should not only identify how many overall requests for cell phone location data law enforcement makes on an annual basis, but also how many requests are made that are not covered by either a warrant, consent, or exigency. A warrant requirement does not impact data obtained by consent or under sufficiently exigent circumstances. See generally, State v. Alston, 88 N.J. 211, 233 (1981) (setting forth test for exigent circumstances exception to warrant requirement); Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (establishing requirements for consent exception to

warrant requirement); State v. Johnson, 68 N.J. 349, 353-54 (1975) (same under State Constitution). Likewise, it should clearly identify specifically how many seizures were made pursuant to court order on less than probable cause.

In sum, where police fail to obtain any judicial process, they cannot legitimately claim to have been prejudiced by the imposition of a "new rule of law," because their actions violated citizens' reasonable expectation that their cell phone location data would not be obtained by law enforcement without justification. Where law enforcement has obtained a court order under the Wiretap Act, retroactive application of the warrant requirement would still serve the new requirement's salutary purpose but would also penalize reasonable reliance on statutory law. And, until further information is provided by the State, the extent of the new rule's impact on the administration of justice is not yet known. However, based on information known to date, the effect is likely to be minimal.

#### POINT III

CELL PHONE USERS HAVE A REASONABLE EXPECTATION OF PRIVACY IN THE LOCATION OF MODERN CELL PHONES NOT ONLY UNDER THE NEW JERSEY CONSTITUTION BUT, LIKELY, ALSO UNDER THE UNITED STATES CONSTITUTION.

Amici submit that this Court's precedent establish New Jersey constitutional privacy interests clearly implicated by cell phone location technology. We respectfully refer the Court to pages 15 through 36 of our main Brief.

Amici submit that modern cell phone location is likely protected under the United States Constitution as well. This issue has yet to be addressed comprehensively by any federal appellate courts. Regardless, it is unnecessary for this Court to decide any federal constitutional question.

The Third Circuit is the only Court of Appeals to consider the issue of whether a warrant may be required for Government acquisition of cell phone location data. It held that a magistrate judge has discretion - to be used sparingly - to require a warrant for disclosure. Otherwise a Court Order is required. In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 315 (3d Cir. 2011).

The most informative federal decision  $\underline{\text{amici}}$  have identified that addresses this question is  $\underline{\text{In re Application of the United States}}$ 

for an Order Authorizing the Release of Historical Cell-Site Information, 809 F.Supp. 2d 113 (E.D.N.Y. 2011). The decision is informative for several reasons. First, there is discussion about the Stored Communication Act as a federal statutory basis for disclosure, along with review of federal constitutional principles relating to the electronic surveillance of location. Id. at 115-19. Second, the court analyzes the federal third-party-disclosure doctrine which, ordinarily, would undermine a reasonable expectation of privacy in users' records held by phone service providers. Third, new technologies are identified, revealing at 120-25. limitations of the doctrine and how a content exception has been developed, thereby extending Fourth Amendment protection to new information technologies such as email, text messaging, and internet Id. at 124-26. Ultimately, the court explains why searches. cumulative cell-site location data is constitutionally protected, thereby requiring a warrant for acquisition. Id. at 126-27.

#### POINT IV

THE CURRENT STATE OF TECHNOLOGY RELATING TO CELL PHONE LOCATION TRACKING ENABLES PINPOINT TRACKING ON A CONTINUOUS BASIS.

The continued research by <u>amici</u> confirms that cell phone location tracking may be performed with pinpoint accuracy on a continuous basis. The facts relating to this technology are taken from the record of non-partisan congressional hearings identifying potential amendments to federal statutes regulating electronic

communications and surveillance. These have been adopted as Findings of Fact in <u>In re Application of the United States of America for Historical Cell Site Data</u>, 747 <u>F.Supp.</u> 2d 827, 831-35 (S.D. Texas 2010), on appeal before the Fifth Circuit ("Texas Opinion"). <u>Amici set forth these facts completely at pages 7 through 14 of their main Brief.</u>

Besides the cell-site and GPS location tracking process discussed in the Texas Opinion, additional technology, if permitted to be used for search and seizure purposes, would now enable law enforcement to track cell phones without the provider's knowledge or involvement. Amici describe these "triggerfish" devices at pages 29 and 30 of their main Brief.

#### CONCLUSION

Amici respectfully submit the within supplemental information in response to the Court's Order, dated November 21, 2012.

Respectfully submitted,

JAVERBAUM WURGAFT HICKS
KAHN WIKSTROM & SININS, P.C.

RUBIN M. SININS, ESQ.

Attorneys for <u>amici</u> <u>curiae</u>, The American Civil Liberties Union of New Jersey Foundation and The Association of Criminal Defense Lawyers of New Jersey

Dated: