ALISON PERRONE

Attorney at Law

P.O. Box 288 Columbus, N.J. 08022 609-298-0615 (phone) 609-298-8745 (fax) aliperr@comcast.net (email)

JOSEPH E. KRAKORA Public Defender Office of the Public Defender 31 Clinton Street P.O. Box 46003 Newark, New Jersey 07101 (973) 877-1200

December 26, 2012

Honorable Chief Justice and Associate Justices of The Supreme Court of New Jersey P.O. Box 970 Trenton, New Jersey 08625

> Re: <u>State v. Thomas W. Earls</u> Docket No. 06875

Your Honors:

This letter is submitted in response to this Court's November 21, 2012, letter requesting additional briefing from the parties. Specifically, this Court asked the parties to address the following questions:

1. If the Court were to determine that a warrant is required to obtain an individual's cell phone location data, would that constitute a "new rule" of law? See State v. Knight, 145 N.J. 238, 250-51 (1996).

This question is addressed in Point One of this letter.

2. If so, should the decision be applied purely prospectively to future cases, to future cases and the pending matter, to future cases and those on direct appeal, or completely retroactively? Id. at 249.

This question is addressed in Point Two of this letter.

3. In considering question number two, please address the three factors that traditionally apply to determining whether a "new rule" is to be applied prospectively or retroactively: [listing factors].

This question is addressed in Point Two of this letter.

4. In responding to question number three, it would helpful to the Court for the State to provide data about the extent to which law enforcement officials rely on cell phone location tracking as an investigative tool. For example, how many requests for cell phone location information, on average, do law enforcement officials make on a monthly or yearly basis?

This question is to be addressed by the State.

5. Please describe the current state of technology relating to cell phone location tracking and similar technologies.

Defendant respectfully refers the Court to the Supplemental Brief of Amicus Curiae Electronic Privacy Information Center, pages 3-16, detailing the current state of technology relating to cell phone location tracking and similar technologies.

6. Do cell phone users today have a reasonable expectation of privacy in the location of modern cell phones under the federal and state constitutions?

This question is addressed in Point Three of this letter. In addition, defendant respectfully refers the Court to pages 12 through 29 of his first supplemental brief.

LEGAL ARGUMENT

POINT ONE

A WARRANT REQUIREMENT FOR THE SEIZURE OF CELL PHONE LOCATION DATA DOES NOT CONSTITUTE A NEW RULE OF LAW. ACCORDINGLY, WERE THIS COURT то DETERMINE THAT Α WARRANT IS OBTAIN AN INDIVIDUAL'S CELL REQUIRED то PHONE LOCATION DATA, THIS DECISION SHOULD BE APPLIED RETROACTIVELY.

A warrant requirement for the seizure of cell phone location data is neither a new rule of law nor a novel concept. For three decades, beginning in <u>State v. Hunt</u>, 91 N.J. 338 (1982), this Court has protected privacy interests in information, like cell phone location data, that individuals disclose for the limited purpose of carrying out "essential activities of today's society." <u>State v. Reid</u>, 194 N.J. 386, 398 (2008). Moreover, as the State acknowledges, the current practice is for police to generally obtain a warrant for the seizure of cell phone location data - a fact which suggests that a warrant requirement for cell phone location data has been largely anticipated by law enforcement in this State. (Psb3; Psb14)¹

Retroactivity under state law is analyzed under a threepart test. "First, we must engage in the threshold inquiry of whether the rule at issue is a 'new rule of law' for purposes of retroactivity analysis." <u>State v. Cummings</u>, 184 N.J. 84, 97

- 3 -

[&]quot;Psb" - State's supplemental brief, dated July 11, 2012.

(2005) (citations and internal quotations omitted). If not new, it will be applied retroactively. "The test for determining whether the rule at issue is a 'new rule of law' is whether a case announces a new rule when it breaks new ground or . . . if the result was not <u>dictated</u> by precedent existing at the time the defendant's conviction became final." Ibid.

To be a new rule, there must be a "sudden and generally unanticipated repudiation of a long-standing practice" and there must be an "appreciable past from which the rule departs." <u>State</u> \underline{v} . Afanador, 151 N.J. 41, 58 (1997) (citations omitted). A decision is not a new rule if it is "not a clear break with the past, but a simple extension of the principle of [prior] cases". State v. Bey, 112 N.J. 123, 213 (1988).

Here, the extension of privacy rights to cell phone location data is merely a logical continuation of wellestablished State constitutional precedent finding a reasonable expectation of privacy in similar data. Thirty years ago, in <u>Hunt</u>, 91 N.J. at 347, this Court "expanded the privacy rights enjoyed by citizens of this state" (<u>State v. Reid</u>, 194 N.J. 386, 397 (2008), by concluding "that telephone toll billing records are "part of the privacy package." <u>Ibid.</u> (quoting <u>Hunt</u>, 91 N.J. at 347). Since <u>Hunt</u>, this Court has continued to restrict law enforcement's unbridled access to the private information that individuals must reveal for the limited purpose of carrying out

- 4 -

the "essential activities of today's society." (<u>Reid</u>, 194 N.J. at 398). This includes bank records, <u>State v. McAllister</u>, 184 N.J. 17, 26-33 (2005); utility records, <u>State v. Domicz</u>, 188 N.J. 285, 299 (2006); and Internet service provider information, Reid, 194 N.J. at 389.

Hence, the extension of privacy protections to cell phone location data was readily foreseeable based on this Court's prior decision in Hunt, McAllister, Domicz, and Reid. Significantly, this Court has consistently refused to apply the federal third-party disclosure doctrine to limit privacy protections in this State. As with toll billing records, bank records, and internet service provider information, cell phone location data is disclosed for the limited purpose of utilizing the service or technology in question. Yet, as this Court explained in the context of phone billing records:

> It is unrealistic to say that the cloak of privacy has been shed because the telephone company and some of its employees are aware of this: information.... This disclosure has been necessitated because of the nature of the instrumentality, but more significantly the disclosure has been made for a limited business purpose and not for release to other persons for other reasons.

<u>Hunt</u>, 91 N.J. at 347. Accordingly, based on this Court's history of granting privacy protections to information similar to cell phone location data, as well as on this Court's steadfast refusal to apply the federal third party disclosure

- 5 -

doctrine to limit such protections, the extension of privacy protections to cell phone location data cannot be considered a new rule of law.

Moreover, it logically follows that while a grand jury subpoena has been found sufficient for the seizure of billing records and Internet service provider information, a subpoena relevancy standard would not be exacting enough to protect individuals from the dramatically intrusive nature of cell phone tracking. Cell phone location data reveals considerably more private information about an individual than billing or service provider records, as cell phone data can reveal not only a person's movements and location, but also a great deal about their values, associations and beliefs. Additionally, cell phone location tracking provides law enforcement with a powerful method of tracking individuals as they traverse between public and private zones. Cell phone location tracking, therefore, is analogous to the more intrusive searches upon which courts have imposed a warrant requirement. See, e.g., Kyllo v. United States, 533 U.S. 27, 34 (2001) (warrant required for thermal imaging of home); United States v. Karo, 468 U.S. 705, 714-15 (1984)(warrant required where electronic tracking device revealed information inside home).

In sum, imposition of a warrant requirement on the seizure of cell phone location information is well-anticipated in this

- 6 -

State. As such, such a requirement would not announce a new rule of law and should therefore be given full retroactive application.

POINT TWO

EVEN IF A WARRANT REQUIREMENT WERE TO CONSTITUTE A NEW RULE OF LAW, IT SHOULD, PURSUANT TO <u>STATE V. KNIGHT</u>, 145 N.J. 238 (1996), BE APPLIED RETROACTIVELY. IN THE ALTERNATIVE, SUCH A REQUIREMENT SHOULD, AT THE VERY LEAST, APPLY TO FUTURE CASES AND THE PENDING MATTER.

As discussed above, the recognition of a privacy right in cell phone location data is not a new rule of law, but rather, is grounded in thirty years of precedent in this State. Even if, however, this Court were to conclude that requiring a warrant for the seizure of cell phone location data were a new rule of law, this requirement should be given full retroactive effect. In the alternative, if this Court were to determine that the warrant requirement should be applied prospectively based on law enforcement's reliance on the Wiretap Act, the warrant requirement should at the very least be applied to the pending matter, in which law enforcement clearly did not rely upon the Wiretap Act.

A new rule of law may be applied in one of the following ways:

- 7 -

make the new rule of law purely (1)prospective, applying it only to cases whose operative facts arise after the new rule is announced; (2) apply the new rule to future and to the parties in the case cases announcing the new rule, while applying the old rule to all other pending and past litigation; (3) grant the new rule limited retroactivity, applying it to cases in (1) and (2) as well as to pending cases where the parties have not yet exhausted all avenues of direct review; and, finally, (4) the new rule complete retroactive give effect, applying it to all cases, even those where final judgments have been entered and all avenues of direct review exhausted.

<u>State v. Nash</u>, 64 N.J. 464, 468-70 (1974). In choosing among those options, courts consider three factors: "(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." <u>State v. Fortin</u>, 178 N.J. 540, 647 (2004) (citing <u>State v. Knight</u>, 145 N.J. 233, 251 (1996)). Importantly, the retroactivity determination often turns on "what is just and consonant with public policy in the particular situation presented." Ibid.

Here, the purpose of protecting privacy rights and remedying constitutional privacy violations supports full retroactive application. Similarly, law enforcement should have, as discussed in Point One, been aware through this Court's long-standing precedent that cell phone location data would be

- 8 -

afforded constitutional protection. And, finally, retroactive application of a warrant requirement would presumably have a negligible impact on the administration of justice according to the State's concession that law enforcement generally obtains a warrant for the seizure of cell phone location data. Accordingly, full retroactive application would be just and consonant with public policy.

While the State will presumably argue for prospective application based on its purported reliance on the procedures set forth in the New Jersey Wiretap Act, this argument is undercut by the State's own admission that law enforcement's current practice is to obtain a warrant, not a grand jury subpoena or court order, prior to seizing an individual's cell phone location data. The New Jersey Wiretap Act, N.J.S.A. 2A:156A-1 et seq., provides an independent statutory basis for judicial oversight prior to law enforcement's seizure of cell location data, delineating four avenues for phone law enforcement to obtain cell phone location information from a cell phone service provider: (1) by securing a warrant; (2) by consent of the subscriber or customer; (3) by court order based on reasonable grounds to believe that the data is relevant and material to an ongoing criminal investigation; and (4) based on a good faith belief of an emergency involving death or serious bodily injury to the subscriber or customer. N.J.S.A. 2A:156A-

- 9 -

1(c). Feasibly, therefore, law enforcement could have reasonably relied upon this statute to seize cell phone location data based on court order, rather than a warrant - a fact which would weigh in favor of prospective application of a warrant requirement. However, according to the State's brief, law enforcement has not been relying upon the court order provision of the Wiretap Act, but rather, has generally been obtaining a warrant - a fact which would weigh in favor of retroactive application of a warrant requirement.

Further, even if the State contends a general reliance on the Wiretap Act, law enforcement clearly did not rely on the Wiretap Act in Mr. Earl's case, where they did not follow any process in obtaining defendant's cell phone location data. Here, law enforcement made three requests of defendant's cell phone provider to release cell phone location data, without seeking a warrant, consent, or a court order.² As such, were this Court to impose a warrant requirement, or any other required process, for the seizure of cell phone location data, this requirement should be, at the very least, applied to defendant's case.

² Moreover, while the Wiretap Act authorizes the seizure of cell phone location information in the event of a lifethreatening emergency, this applies only "the location information for a <u>subscriber's or customer's mobile or wireless</u> <u>communications device</u>" 2A:156A-29c(4) (emphasis supplied). Here, police sought defendant's location information, not the subscriber, Gates', location information.

POINT THREE

CELL PHONE USERS TODAY HAVE A REASONABLE EXPECTATION OF PRIVACY IN THE LOCATION OF MODERN CELL PHONES UNDER THE FEDERAL AND STATE CONSTITUTIONS.

Defendant respectfully refers the Court to his first supplemental brief, pages 12 to 29, for a discussion of State precedent establishing a reasonable expectation of privacy in the location of modern cell phones.

With respect to whether cell phone users today have a reasonable expectation of privacy under federal law, defendant submits that although this issue has not yet been squarely addressed by any federal courts, it is likely that federal courts will ultimately recognize a reasonable expectation of privacy in the location of modern cell phones. Although, as discussed in defendant's first supplemental brief, the Knotts and Karo line of federal cases rely upon distinctions between public and private realms, and the United States Supreme Court's more recent decision in Jones relies upon an antiquated trespass theory, modern cell phone technology has blurred the line between public and private realms as this technology can be used to monitor an individual's movements in and out of public and private areas over a period of time, and this can be accomplished without the type of physical intrusion into person or property contemplated by Jones. In light of the Supreme

- 11 -

Court's admonition that "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish," <u>Kyllo</u>, 533 U.S. 27, 34 (2001), and for the reasons discussed in defendant's first supplemental brief, it is likely that federal courts, recognizing the degree of privacy encroachment posed by cell phone location tracking, will require that acquisition of cell phone data be subject to the warrant requirement and that suppression be the remedy for the failure to obtain a warrant.

CONCLUSION

In all other respects, defendant relies upon his Appellate Division brief and first Supreme Court supplemental brief. For the above stated reasons and for the reasons set forth in defendant's Appellate Division brief and first Supreme Court supplemental brief, the denial of defendant's motion to suppress must be reversed.

Respectfully submitted,

JOSEPH E. KRAKORA Public Defender Attorney for Defendant-Petitioner

BY:

ALISON PERRONE Designated Counsel