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

STATE OF NEW JERSEY,	CRIMINAL ACTION
<pre>Plaintiff-Respondent, v.</pre>	On Appeal From a Final Order of the Superior Court, Appellate Division, Affirming the Judgment of Conviction.
THOMAS W. EARLS,	<u>Sat Below</u> :
Defendant-Appellant.	Hon. Anthony J. Parrillo, J.A.D. Hon. Stephen Skillman, J.A.D. Hon. Patricia B. Roe, J.A.D.

BRIEF OF <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

Attorneys for ACDL-NJ

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	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
<i>On the Brief:</i> Rubin M. Sinins, Esq.	Jeffrey S. Mandel, Esq. PinilisHalpern, LLP 160 Morris Street Morristown, NJ 07960 (973) 401-1111 jmandel@pinilishalpern.com

TABLE OF CONTENTS

Page

TABLE OF (CONTEI	NTS	i
TABLE OF 2	AUTHO	RITIES	iii
STATEMENT	OF II	NTEREST	1
PRELIMINA	RY STA	ATEMENT	4
PROCEDURA	L HIST	IORY	5
STATEMENT	OF FZ	ACTS	б
<u>ARGUMENT</u>			
POIN	<u>r i</u> :	Under the New Jersey Constitution, There Is A Reasonable Expectation of Privacy In Cell Phone Location Information.	15
Α.	This tiona Impl:	Court's Precedents Establish Constitu- al Privacy Interests That Are Clearly icated By Cell Phone Location Technology.	15
В.	Curre tutio tatio	ent Statutory, Commercial, and Consti- onal Protections Underscore the Expec- on of Privacy in Cell Phone Location.	20
	1.	Statutory Protections	20
	2.	Cell Phone Customer Agreements and Privacy Policies	24
	3.	Constitutional Privacy Interest in Tracking Technology	26
С.	Neith Corre tiona	ner the Appellate Division Nor the State ectly Gauges the Substantial Constitu- al Threat to Privacy Cell Phone Tracking	
	Poses	5.	31
	1.	The Appellate Division Decision	31
	2.	The State's Position	34

<u>point ii</u> :	Law Enforcement Acquisition of Cell Phone Location Information Should Require a Warrant Supported by Probable Cause and Particularity.	37
<u>POINT III</u>	: Suppression is the Proper Remedy for Law Enforcement's Improper Acquisition of Cell Phone Location Information	41
CONCLUSION		11
CONCHORION		44

TABLE OF AUTHORITIES

CASES	Page	e(s)
<u>A.A. ex rel. B.A. v. Attorney General of</u> <u>New Jersey</u> , 189 N.J. 128 (2007)		1
<u>California v. Greenwood</u> , 486 U.S. 35,37 (1988)		28
<u>Casey v. Male</u> , 63 N.J. Super. 255, 259 (Co. Ct. 1960)		3
<u>Devega v. State</u> , 689 S.E. 2d 294, 300 (Ga. 2010)		32
<u>Doe v. Poritz</u> , 142 N.J. 1, 87 (1995)	16,	27
<u>In re Application for Pen Register and</u> <u>Trap/Trace Device with Cell Site Location</u> <u>Authority</u> , 396 F. Supp. 2d 294, 295 (E.D.N.Y. 2005)		40
<u>In re Application for Pen Register and</u> <u>Trap/Track Device with Cell Site Location</u> <u>Authority</u> , 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005)		40
<u>In re Application for the Installation</u> <u>and Use of a Pen Register</u> , 439 F. Supp. 2d 456, 457 (D. Md. 2006)		40
<u>In re Application of the United States</u> <u>for an Order Authorizing the Disclosure</u> <u>of Prospective Cell Site Information</u> , 412 F. Supp. 2d 947, 949 (E.D. Wis. 2006)		40
<u>In re Application of the United States</u> <u>for an Order Directing a Provider of</u> <u>Electronic Communication Service to</u> <u>Disclose Records to the Government</u> , 620 F. 3d 304, 315 (3d Cir. 2011)		40
<u>In re Application of the United States</u> <u>for an Order Relating to Target Phone 2</u> , 733 F. Supp. 2d 939, 941 n.1 (N.D. Ill. 2009)		40

<u>In re Application of the United States</u> of America for Historical Cell Site Data,				
747 F. Supp. 2d 827, 831-35 (S.D. Texas 2010)	б,	7-14,	16,	40
<u>Joye v. Hunterdon Central Req'l High</u> <u>School Brd. Of Ed.</u> , 176 N.J. 568 (2003)				1
<u>Katz v. United States</u> , 389 U.S. 347, 351 (1967)				27
<u>Kyllo v. United States</u> , 533 U.S. 27, 36 (2001)		26,	29,	32
<u>Maryland v. Macon</u> , 472 U.S. 463, 468 (1985)				19
<u>NAACP v. Alabama</u> , 357 U.S. 449, 461 (1958)				19
<u>People v. Weaver</u> , 909 N.E. 2d 1195, 1196- 97 (N.Y. 2009)				28
<u>Roberts v. U.S. Jaycees</u> , 468 U.S. 609, 617-18 (1984)			18	-19
<u>See v. City of Seattle</u> , 387 U.S. 541, 543 (1967)				26
<u>Stanford v. Texas</u> , 379 U.S. 476, 484-85 (1965)				19
<u>State v. Badessa</u> , 185 N.J. 303, 311 (2005)				41
<u>State v. Best</u> , 201 N.J. 100 (2010)				1
<u>State v. Buda</u> , 195 N.J. 278 (2008)				2
<u>State v. Byrd</u> , 198 N.J. 319 (2009)				2
<u>State v. Campbell</u> , 759 P. 2d 1040, 1048 (Or. 1988)				28
<u>State v. Carty</u> , 170 N.J. 632 (2002)				1
<u>State v. Chun</u> , 194 N.J. 54 (2008)				2

<u>State v. Cottle</u> , 194 N.J. 449 (2008)			2
<u>State v. Domicz</u> , 188 N.J. 285, 297-301 (2006)		15	-16
<u>State v. Earls</u> , 420 N.J. Super. 583, 599 (App. Div. 2011)		31,	32
<u>State v. Evers</u> , 175 N.J. 355, 374 (2003)	41,	42,	43
<u>State v. Frankel</u> , 179 N.J. 586 (2004)			1
<u>State v. Gadsden</u> , 303 N.J. Super. 491, 505 (App. Div.), <u>certif. denied</u> , 152 N.J. 187 (1997)			41
<u>State v. Hempele</u> , 120 N.J. 182, 215 (1990)) 16,	20,	28
<u>State v. Henderson</u> , 208 N.J. 208 (2011)			2
<u>State v. Hunt</u> , 91 N.J. 338, 345-48 (1982)	15,	16,	20
<u>State v. Hupka</u> , 203 N.J. 222 (2010)			2
<u>State v. Jackson</u> , 76 P. 3d 212, 223-24 (Wash. 2003)			28
<u>State v. J.G.</u> , 201 N.J. 369 (2010)			2
<u>State v. Marquez</u> , 202 N.J. 485 (2010)			2
<u>State v. McAllister</u> , 184 N.J. 17, 19 (2005)		15,	20
<u>State v. Mollica</u> , 114 N.J. 329 340-45 (1989)			15
<u>State v. Nunez-Valdez</u> , 200 N.J. 129 (2009)			2
<u>State v. Nyhammer</u> , 197 N.J. 383 (2009)			2
<u>State v. Osorio</u> , 199 N.J. 486 (2009)			2
<u>State v. Ravotto</u> , 169 N.J. 227 (2001)			2

<u>State v. Reid</u> , 194 N.J. 386 (2008)	1, 2, 15, 41, 42	17-18,	20,	38,
<u>State v. Rivera</u> , 205 N.J. 472 (2011)				2
<u>State v. Rose</u> , 206 N.J. 141 (2011)				2
<u>State v. Schmidt</u> , 206 N.J. 71 (2011)				2
<u>State v. Sweet</u> , 195 N.J. 357 (2008)				2
<u>State v. W.B.</u> , 205 N.J. 588 (2011)				2
<u>State ex rel. J.A.</u> , 195 N.J. 324 (2008)				2
<u>State ex rel. P.M.P.</u> , 200 N.J. 166 (2009	9)			2
<u>State in the interest of J.G., N.S.</u> <u>and J.T.</u> , 151 N.J. 565 (1997)				2
<u>Stone v. State</u> , 941 A. 2d 1238, 1250 (Md. Ct. Spec. App. 2008)				32
<u>Stoner v. California</u> , 376 U.S. 483, 486 (1964)				26
<u>Taxpayers Ass'n. of Weymouth Twp. v.</u> <u>Weymouth Twp.</u> , 80 N.J. 6, 17 (1976), <u>cert. denied</u> , 430 U.S. 977 (1977)				3
<u>United States v. Booker</u> , 543 U.S. 220 (2005)				29
<u>United States v. Forest</u> , 355 F.3d 942, 951 (6 th Cir. 2004)			29,	32
<u>United States v. Jones</u> , 565 U.S (2012)		19,	26,	27
<u>United States v. Garcia</u> , 474 F.3d 994, 998 (7 th Cir. 2007)				29
<u>United States v. Karo</u> , 468 U.S. 705 (1984)			26,	32
<u>United States v. Knotts</u> , 460 U.S. 276 (1983)			26,	32

<u>United States v. Maynard</u> , 615 F.3d 544, 563 (D.C. Cir. 2010) aff/d Jones	
565 U.S (2012)	27, 29, 38
<u>United States v. Torres</u> , 751 F. 2d 875, 883-84 (7 th Cir. 1984)	38
RULES	
<u>N.J.R.E.</u> 201	6
<u>R.</u> 3:5-2	37
<u>R.</u> 3:5-3	37
<u>STATUTES</u>	
18 U.S.C. §§2701-2711 (2010)	23
18 U.S.C. §2703(c)(1)	23, 41
18 U.S.C. §3121	23, 41
47 U.S.C. §222(f)	22-23
47 U.S.C. §1002(a)(2)(B)	23
N.J.S.A. 2A:156A-1 <i>et seq</i> .	20
N.J.S.A. 2A:156A-2w	22
N.J.S.A. 2A:156A-9(c)	38
N.J.S.A. 2A:156A-21	42
N.J.S.A. 2A:156A-24	42
N.J.S.A. 2A:156A-29	21-22, 37
N.J.S.A. 2A:156A-29c	41, 42

OTHER AUTHORITIES

Curtis, William, <u>Triggering a Closer Review:</u> <u>Direct Acquisition of Cell Site Location</u> Tracking Information and the Argument for	
Consistency Across Statutory Regimes, 45	
Columbia J.L. & Soc. Probs. 139 (Fall 2011)	30
Kothari, Vivek, <u>Autobots, Decepticons and</u> <u>Panopticons: The Transformative Nature of</u> <u>GPS Technology and the Fourth Amendment</u> , 6 Crim. L. Brief 37, 45 (2010)	19
LaFave, Wayne R., Search and Seizure: A Treatise on the Fourth Amendment § 1.5(c) (3d ed. 1996 & Supp. 2003)	41
Sanchez, Julian, FOIA Docs Show Feds Can Lojack Mobile Without Telco Help, ARS TECHNICA (Nov. 16, 2008), http://arstechnica.com/ tech-policy/news/2009/11/foia-doc-show-feds-can- lojack-mobiles-without-telco-help-ars	30
'Stingray' Phone Tracker Fuels Constitutional Clash, Sept. 22, 2011, http://online.wsj.com/ article/SB10001424 05311190419460457658311272 3197574.html	30
U.S. Dept. of Justice, Electronic Surveillance Manual 38-40 (2005)	30
http://att.com/gen/privacy-policy?pid=2506	24
http://foursquare.com/privacy	25
http://google.com/mobile/latitude	25
http://www.ctia.org/business_resources /wic/index/AID/11300	25
http://www.sprint.com/legal/privacy.html	24
http://www.t-mobile.com/company/website/ privacypolicy.aspx	24
http://www22.verizon.com/privacy	24

18 Pa. Cons. Stat. §5761	38
Fla. Stat. §§934.06	37
Fla. Stat. §§934.42	37
Haw. Rev. Stat. §§803-42	38
Haw. Rev. Stat. §§803-44.7	38
Minn Stat. §§626A.37	37
Minn Stat. §§626A.3.5	37
Okla. Stat. Ct. 13, §§126-6	38
Okla. Stat. Ct. 13, §§177.6	38
S.C. Code Ann. §10-30-140	37
Utah Code Ann. §§77-23a-4	37
Utah Code Ann. §§77-23a-7	37
Utah Code Ann. §§77-23a-15.5	37

STATEMENT OF THE INTEREST OF AMICI

American Civil Liberties Union of New Jersey

The American Civil Liberties Union of New Jersey (ACLU-NJ) is a private, non-profit, non-partisan membership organization dedicated to the principle of individual liberty embodied in the Constitution. Founded in 1960, the ACLU-NJ has approximately 15,000 members and supporters in New Jersey. The ACLU-NJ is the state affiliate of the American Civil Liberties Union, which was founded in 1920 for identical purposes, and is composed of approximately 500,000 members and supporters nationwide.

The ACLU-NJ strongly supports ensuring protections against unreasonable searches and seizures for all persons and has participated as <u>amicus curiae</u> or direct counsel in numerous such cases. <u>See</u>, <u>e.q.</u>, <u>State v. Best</u>, 201 N.J. 100 (2010) (challenging special needs searches in school parking lots); <u>State v. Reid</u>, 194 N.J. 386 (2008) (finding expectation of privacy in Internet Service Provider records); <u>A.A. ex rel. B.A. v. Attorney General of New Jersey</u>, 189 N.J. 128 (2007) (challenging DNA testing of juvenile offenders); <u>State v. Frankel</u>, 179 N.J. 586 (2004) (determining parameters of emergency aid doctrine); <u>Joye v. Hunterdon Central</u> <u>Req'l High School Brd. Of Ed.</u>, 176 N.J. 568 (2003) (challenging random student drug testing); <u>State v. Carty</u>, 170 N.J. 632 (2002) (State Constitution requires reasonable suspicion of criminal activity prior to police seeking consent to search lawfully stopped

motor vehicle); <u>State v. Ravotto</u>, 169 N.J. 227 (2001) (police used unreasonable force in obtaining a blood sample from a DWI suspect where suspect had consented to breathalyzer test); <u>State in the</u> <u>interest of J.G., N.S. and J.T.</u>, 151 N.J. 565 (1997) (challenging requirement of HIV/AIDS test for those charged with sexual assault).

Association of Criminal Defense Lawyers of New Jersey

The Association of Criminal Defense Lawyers of New Jersey (ACDL-NJ) is comprised of over 400 members of the criminal defense bar of this State. Members of the Association include attorneys in private practice and public defenders. The ACDL-NJ has participated as <u>amicus</u> <u>curiae</u> in numerous matters before this Court. See, e.g., State v. Henderson, 208 N.J. 208 (2011); State v. Rose, 206 N.J. 141 (2011); State v. Schmidt, 206 N.J. 71 (2011); State v. W.B., 205 N.J. 588 (2011); State v. Rivera, 205 N.J. 472 (2011); State v. Hupka, 203 N.J. 222 (2010); State v. Marquez, 202 N.J. 485 (2010); State v. J.G., 201 N.J. 369 (2010); State ex rel. P.M.P., 200 N.J. 166 (2009); State v. Nunez-Valdez, 200 N.J. 129 (2009); State v. Osorio, 199 N.J. 486 (2009); State v. Byrd, 198 N.J. 319 (2009); State v. Nyhammer, 197 N.J. 383 (2009); State v. Sweet, 195 N.J. 357 (2008); State ex rel. J.A., 195 N.J. 324 (2008); State v. Buda, 195 N.J. 278 (2008); State v. Cottle, 194 N.J. 449 (2008); State v. Reid, 194 N.J. 386 (2008); State v. Chun, 194 N.J. 54 (2008).

The ACDL-NJ chooses very carefully those cases in which it seeks to appear as <u>amicus curiae</u>. Although the ACDL-NJ receives many requests for assistance, it deliberately restricts its participation as <u>amicus curiae</u> to those cases which present issues crucial to the rights of criminal defendants and to the fair administration of the criminal justice system.

The privacy issues implicated by this case are of particular significance to the criminal defense bar and citizens of this State. Such issues include whether there is a reasonable expectation of privacy under the State Constitution in cell phone location information; whether law enforcement acquisition of cell phone location information should require a warrant; and whether suppression is the proper remedy for law enforcement's improper acquisition of cell phone location information.

The participation of <u>amici curiae</u> is particularly appropriate in cases with "broad implications," <u>Taxpayers Ass'n. of Weymouth</u> <u>Twp. v. Weymouth Twp.</u>, 80 N.J. 6, 17 (1976), <u>cert. denied</u>, 430 U.S. 977 (1977), or in cases of "general public interest." <u>Casey v.</u> <u>Male</u>, 63 N.J. Super. 255, 259 (Co. Ct. 1960) (history and parameters of <u>amicus curiae</u> participation). This is such a case, as it raises far-reaching questions of privacy protections in a changing technological world.

PRELIMINARY STATEMENT

This Court must decide whether a cell phone user has a constitutional right of privacy in his location. Here the police, three times in one day, requested and acquired real-time cell phone location information from defendant's provider. They did so without a warrant, court order or other judicial authorization. The question is whether the New Jersey Constitution protects this cell phone location information and limits law enforcement's acquisition of it.

Cell phone services allow providers to record and collect location information. This practice turns a cell phone into a powerful tracking device. In seeking to locate individuals who may be targets or witnesses in criminal investigations, police have attempted to obtain this information in order to track a user's location in real-time. Police investigators may also seek historical location information to trace users' past locations. Cell phone providers have users' real-time and historical location records.

Established state constitutional principles, existing statutes and provider privacy policies all support the proposition that cell phone users have a reasonable expectation of privacy in their cell phone location information. Indeed, if disclosed, that information vitiates individual privacy, inhibits movement and compromises associations. Thus, users expect providers to keep their real-time

and past locations private, and not disclose them on demand to police.

<u>Amici</u> urge the Court to reverse the Appellate Division in the present case, which analyzed the matter incorrectly and failed to recognize the privacy interests at stake. <u>Amici</u> further urge the Court to require a warrant, supported by probable cause and particularity, before police can obtain cell phone location information. Indeed, absent a constitutionally based warrant requirement, police could use cell phone location information to conduct comprehensive, unrestricted surveillance. That would be an intolerable infringement on individuals' civil liberties.

Finally, <u>amici</u> posit that when police obtain cell phone location information unconstitutionally, or illegally through defective process, suppression is the only remedy that vindicates principles of deterrence and judicial integrity. Current statutory civil remedies do not protect defendants who otherwise face use of improperly-obtained evidence in criminal proceedings.

PROCEDURAL HISTORY

<u>Amici</u> adopt the procedural history in the parties' briefs.

STATEMENT OF FACTS

Amici adopt the Statement of Facts in the parties' briefs.

Additionally, because the record does not include facts concerning the relevant cell phone location technology, <u>amici</u> suggest the Court adopt and rely on the Findings of Fact in <u>In re</u> <u>Application of the United States of America for Historical Cell</u> <u>Site Data</u>, 747 F. Supp. 2d 827, 831-35 (S.D. Texas 2010), on appeal before the Fifth Circuit ("Texas Opinion"); <u>See N.J.R.E.</u> 201 (Judicial Notice of Law and Adjudicative Facts). These Findings of Fact are taken from the record of non-partisan congressional hearings identifying potential amendments to federal statutes regulating electronic communications and surveillance. <u>Id.</u> at 830.

These facts will help the Court understand the applicable technology and allow it to consider the constitutional question in proper context. As the Texas Opinion notes: "[C]ase law developments have been outstripped by advancing technology," which has "altered the legal landscape even more profoundly than the new case law." <u>Id.</u> For the Court's convenience, this brief reproduces the Texas Opinion's Findings of Fact. The court's citations are omitted.

Findings of Fact

Cell Phone Technology in General

1. Unlike conventional wireline telephones, cellular telephones use radio waves to communicate between the user's handset and the telephone network.

2. Cellular service providers maintain networks of radio base stations ("cell sites") spread throughout their geographic coverage areas.

3. A wireless antenna at each cell site detects the radio signal from the handset, and connects it to the local telephone network, the Internet, or another wireless network.

4. Cell phones periodically identify themselves to a nearby base station as they move about the coverage area, a process called "registration." The registration process is automatic, and occurs whenever the phone is on, without the user's input or control. The registration signal is carried over a channel separate from the channel used to carry the call itself.

5. During a call, if the phone moves nearer to another base station, the call is "handed off" between base stations without interruption.

6. No longer just big three-sided radio towers, base station antennas can be mounted outdoors on roof-tops, building-sides, trees, flagpoles, and church steeples, or indoors in homes and offices. Many are no larger than a conventional stereo speaker.

Wireless Location Technology

7. There are two distinct technological approaches for fixing the location of a cell phone: handset-based (GPS) and network-based (cell site).

8. GPS is the acronym for Global Positioning System, which is comprised of at least 24 satellites constantly orbiting the earth in six low earth orbits.

9. For GPS location, special hardware in a user's handset receives signals from at least four global position satellites, allowing the handset to calculate its latitude and longitude whenever it is unobstructed satellite range.

10. Current GPS technology can archive spatial resolution typically within ten meters.

11. Despite its relative precision, GPS has at least three fundamental drawbacks as a location tool: (a) it is not available for all handset models, especially older models; (b) it works reliably only outdoors, when the handset has an unobstructed view of several GPS satellites in the sky above; and (c) perhaps most significantly, it can be disabled by the user.

12. For these reasons, GPS is neither the most pervasive nor the most generally applicable phone location system, especially for surveillance purposes.

13. For network-based location, the position of the phone is calculated by the network based on data collected and analyzed a the cell site receiving the phone's signals, without explicit assistance from the user or his handset.

14. A variety of techniques may be used for network-based location. The most basic technique is to identify the particular base station (or sector) with which the phone was communicating ever time it makes or receives a call and when it moves from one sector to another. 15. The relative precision of cell site location depends on the size of the cell sector. The smaller the sector, the more precise the location fix.

16. In early cellular systems, base stations were placed as far apart as possible to provide maximum coverage. At that time, a sector might cover an area several miles or more in diameter. Today this is true only of sparsely populated, rural areas.

17. Due to a combination of factors, the size of the typical cell sector has been steadily shrinking in recent years.

18. As the density of cellular users grows in a given area, the only way for a carrier to accommodate more customers is to divide the coverage area into smaller and smaller sectors, each served by its own base station and antenna.

19. New services such as 3G Internet create similar pressure on the available spectrum bandwidth, again requiring a reduction in the geographic size of sectors

20. Another factor contributing to smaller sector size is consumer demand for more reliable coverage in areas with unfavorable radio conditions (*e.g.*, elevators), which again requires additional base stations to cover such "dead spots."

21. The number of cellular base stations in the U.S. has tripled over the last decade, and the rate of growth is accelerating. By one industry estimate, there are now over 251,000 reported cell sites operating in the United States. There were only 913 the year before ECPA was passed.

22. The trend toward smaller cell sectors has accelerated with the deployment of smaller-scale base stations designed to serve very small areas such as particular floors of buildings, or individual homes and offices. 23. This new generation of cellular base station is generally known as a "micorcell," and smaller versions are sometimes referred to as a "picocell" or "femtocell."

24. Microcell technology is increasingly used by many carriers, including AT&T, Verizon, and Sprint. A microcell has a range of 40 feet (12 meters).

25. The effect of this trend toward smaller sectors is that knowing the base station (or sector ID) handling a call is tantamount to knowing the user's location to within a relatively small geographic area. In urban areas and other environments that use microcells, this area can be small enough to identify individual floors and rooms within buildings.

26. The decreasing size of cell sectors is not the only factor making network-based location more accurate. New technology allows providers to locate not just the sector in which the phone is located, but also its position within the sector.

27. By correlating the precise time and angle at which a phone's signal arrives at multiple sector base stations, a provider can pinpoint the phone's latitude and longitude to an accuracy within 50 meters or less. Emerging versions of the technology are even more precise.

28. Such enhanced location technologies are commercially available, and many carriers contract with specialized companies that provide "off the shelf" location-based products and system upgrades.

29. Many of these companies were formed in response to directives from Congress and the FCC to develop wireless location technology in order to enhance the nation's emergency response (E-911) system.

Data Collection and Retention

30. Cell location information is quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the target user.

31. Carriers typically create "call detail records" that include the most accurate location information available to them.

32. Historically, before more advanced location techniques were available, carrier call detail records typically included only the cell sector or base station identifier that handled the call. Today, the base station or sector identifier carries with it more locational precision that it once did.

33. As even more precise location information becomes available, call detail records can now include the user's latitude and longitude along with the sector ID data. Some carriers also store frequently updated, highly precise, location information not just when calls are made or received, but as the device moves around the network.

34. The cost of collecting and storing high resolution location data about every customer has become much cheaper in the last few years. Such information is valuable for network management, marketing, and developing new services. This trend toward greater and more extensive data archives is likely to continue.

35. Some carriers effectively outsource the task of collecting, analyzing, and storing location information to companies offering specialized location technology.

36. One such company installs multiple auxiliary receivers (called "Location Measurement Units", or LMUs) on existing cell towers and base stations to enhance location accuracy. These auxiliary receivers are very accurately time-synchronized to each other, and very sensitive; at any given moment, a single handset may be in communication with 30 or more LMUs.

37. This same company has deployed over 100,000 LMU's.

38. The company not only transmits this detailed location information to the carrier, it can also manage and analyze historic location and calling activity data. Such data can also be organized and aggregated to reflect current user activities, mobile events, and interactions with other devices.

39. Most carrier systems use a variety of large and small sector configurations. A mobile user, in the course of her daily movements, will periodically move in and out of large and small sectors. The locational precision of cell sector data recording those movements will vary widely over the course of a given day, from relatively less to relatively very precise.

40. Neither the user nor the carrier can predict how precise the next location data will be. For a typical user, over time, some of that data will likely have locational precision similar to that of GPS.

41. Given these advances in technology, it is no longer valid to assume that network cell sector records will yield only as approximate user location.

42. As cellular network technology evolves, the traditional distinction between "high accuracy" GPS tracking and "low accuracy" cell site tracking is increasingly obsolete, and will soon be effectively meaningless.

Cell Phone Use Statistics

43. Today there are more than 285 million active wireless subscriber accounts in the United States. Many households no longer have traditional "landline" telephone service, opting instead for cellular phones carried by each family member.

44. Cell phones are frequently used in the home or in other places not open to public view: one study shows that at least 52% of cell phone calls are made indoors; another study indicates that two out of three adults sleep with their cell phone nearby.

45. In 1999, the number of reported wireless minutes of use was less than 200 billion. A decade later, the number has grown to more than 2.2 *trillion* minutes.

46. Over the same decade, the annual number of text messages has jumped to 1.56 trillion.

47. According to a 2008 Nielsen survey, the average U.S. cell phone user made or received 204 voice calls every month. A 2010 Pew Research study of adult cell phone use shows that the median number of voice calls for a typical user is 5 per day, while the average (mean) is 13.1 calls/day. This study also shows that African American and Hispanic cell users make more calls (and texts) on average than their white counterparts.

48. Similar patterns are reflected in cell phone texting. The 2008 Nielsen survey reported the average cell phone user made or received 357 text messages a month. According to the 2010 Pew Research study, adults send and receive a median of 10 texts daily; the average (mean) is 39.1 texts/day. Both figures are more than double the levels reported by Pew just 8 months earlier in September 2009. Teen use of text messaging is substantially heavier: the teen median level is 50 texts daily, and the mean is 112.4. 49. Based on these numbers, even if limited to the beginning and end of actual phone calls and text messages, cell site data for a typical adult user will reveal between 20 and 55 location points a day. This data is sufficient to plot the target's movements hour by hour for the duration of the 60 day period covered by the government's request.

50. If registration data were also collected by the provider and made available, as the Government has requested, such records would track the user on a minute by minute basis, compiling a continuous log of his life, awake and asleep, for a two month period.

[<u>Id.</u> at 831-35 (emphasis in original).]

ARGUMENT POINT I

UNDER THE NEW JERSEY CONSTITUTION, THERE IS A REASONABLE EXPECTATION OF PRIVACY IN CELL PHONE LOCATION INFORMATION.

A. This Court's Precedents Establish Constitutional Privacy Interests That Are Clearly Implicated By Cell Phone Location Technology.

This Court's prior privacy decisions mandate a a holding that the New Jersey Constitution protects cell phone location information. The Appellate Division failed to recognize this constitutional privacy interest; instead, it relied on inapposite decisions that do not consider how cell phone location technology threatens privacy interests.

As this Court has definitively held, an individual does not lose his right to privacy merely because information is in the hands of a third party. <u>State v. Reid</u>, 194 N.J. 386, 399 (2008) (disclosure of information to a third-party provider, as an essential step to obtaining service, "does not upend the privacy interest at stake"). Thus, for example, internet service provider (ISP) subscriber information is constitutionally protected. <u>Id.</u> Telephone billing records, call records and bank records are likewise constitutionally protected. <u>State v. Hunt</u>, 91 N.J. 338, 345-48 (1982); <u>State v. Mollica</u>, 114 N.J. 329 340-45 (1989); <u>State v. McAllister</u>, 184 N.J. 17, 19 (2005). <u>See also State v. Domicz</u>,

188 N.J. 285, 297-301 (2006) (acknowledging possible expectation of privacy in utility records); <u>State v. Hempele</u>, 120 N.J. 182, 215 (1990) (expectation of privacy in curbside trash). This Court has further recognized a general constitutional right of privacy in the compilation and dissemination of information that may otherwise be available only in scattered forms. <u>Doe v. Poritz</u>, 142 N.J. 1, 87 (1995).

As this Court explained in Hunt:

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.

[91 N.J. at 347.]

These precedents support finding a constitutional privacy interest in cell phone location information. Here, that information is cell-site data, pinpointing the nearest cell tower at a given time. As the Texas Opinion makes clear, this location information can be very precise, and now approaches the accuracy of GPS tracking. 747 F. Supp. 2d at 834 (Finding of Fact 42). The cell-site location is essential for the provision of services. Yet, due simply to the manner in which cell phones function, the result is that it also operates as a tracking mechanism for the cell phone user. As the trial court here recognized, "[w]hile the

cell phone was not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell site data." 4T19-13.¹

Like the protected ISP information, toll-billing and bank records, cell phone location information is "integrally connected to essential activities of today's society." <u>Reid</u>, 194 N.J. at 398. Indeed, this Court's reasoning in protecting ISP records applies with even greater force to cell phones:

> [I]t is hard to overstate how important computers and the Internet have become to everyday, modern life. Citizens routinely access the Web for all manner of daily activities: to gather information, explore ideas, read, study, shop, and more.

> Individuals need an ISP address in order to access the Internet. However, when users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential. Many are unaware that a numerical IP address can be captured by the websites they visit.... Only an Internet service provider can translate an IP address into a user's name.

> In addition, while decoded IP addresses do not reveal the content of Internet communications, subscriber information alone can tell a great deal about a person. With a complete listing of IP addresses, one can track a person's Internet usage.... Such information can reveal intimate

¹ In this case, police requested the real-time location tracking of a cell phone. Real-time information can locate people contemporaneously and can provide evidence in criminal trials. But it is only one investigative function of cell phone tracking. Police may also seek historical location data. Historical location information may also be evidential. For example, police could use historical data to reconstruct a target's movement over time, or at the time of a past crime.

details about one's personal affairs in the same way disclosure of telephone billing records does. Although the contents of Internet communications may be even more revealing, both types of information implicate privacy interests.

[<u>Id.</u> at 398-99.]

The same is true for cell phones. Cell phone use may be more ubiquitous than Internet use.

Cell phone location information can reveal intimate details of one's affairs. Cell phone location information reveals not only location, but also movement and associations. Significantly, location information can reveal people's presence in protected locations like their home or office, and can reveal their doctors' visits, shopping habits, attendance at church, or association with others. The information, significantly, includes not only public movement, but private locations people enter. Discerning a user's location on even a single occasion can reveal intimate location information. This same location information over time – historical information – reveals even more about a user's movements, actions and associations.

Besides one's privacy interest in location and movement, cell phone location tracking - particularly if prolonged - may implicate one's First Amendment right of association. The constitutional right to freedom of association protects against state intrusion into the "choices to enter into and maintain certain intimate human relationships." <u>Roberts v. U.S. Jaycees</u>, 468 U.S. 609, 617-18

(1984). Government action discouraging and potentially limiting the free exercise of First Amendment protections is also proscribed. <u>NAACP v. Alabama</u>, 357 U.S. 449, 461 (1958). <u>See</u> Vivek Kothari, Autobots, Decepticons and Panopticons: The Transformative Nature of GPS Technology and the Fourth Amendment, 6 Crim. L. Brief 37, 45 (2010) ("[M]ore than mere locations, GPS devices provide an index of known associates and associations and insight into the frequency of those associations.") "Awareness that the Government may be watching chills associational and expressive freedoms." United States v. Jones, 565 U.S. ___ (2012) (Sotomayor, J., concurring). Accordingly, the Fourth Amendment warrant requirement should be accorded "scrupulous exactitude" when First Amendment concerns are implicated. See Stanford v. Texas, 379 U.S. 476, 484-85 (1965); Maryland v. Macon, 472 U.S. 463, 468 (1985). The Court should recognize that cell phone technology significantly implicates these privacy and associational interests.

Cell phone users do not intend to disclose their location simply by using the phone. As with Internet users, cell phone users do not knowingly and voluntarily assume the risk of having their location information revealed to the public. Cell phone location information is not data the user directly conveys to make a call. Rather, that information is generated and recorded automatically. There is no reason to believe individuals even realize their cell phone provider records their location

information. As with the information at issue in <u>Reid</u>, <u>Hunt</u>, and <u>McAllister</u>, cell phone location information is information that people recognize the cell phone company must obtain for the purpose of providing service, but that they nevertheless reasonably expect will otherwise be protected and not be subject to disclosure to the government.

B. Current Statutory, Commercial, and Constitutional Protections Underscore The Expectation of Privacy in Cell Phone Location Information.

The New Jersey Constitution protects individuals' reasonable expectations of privacy. This Court has determined that "[e]xpectations of privacy are established by general social norms." <u>Hempele</u>, 120 N.J. at 200 (quotation reference omitted).

Simply put, individuals expect privacy in location information held by cell phone providers. Current statutory and constitutional provisions, as well as providers' privacy policies, establish the reasonableness of that expectation.

1. <u>Statutory Protections</u>

First, statutory protections for cell phone location information – provisions that limit access by law enforcement – confirm a reasonable expectation of privacy. Both state and federal law restrict law enforcement's ability to acquire cell phone location information.

The Wiretapping and Electronic Surveillance Control Act, N.J.S.A. 2A:156A-1 *et seq*. ("New Jersey Wiretap Act") provides:

2A:156A-29. Requirements for access.

* * *

c. A provider of electronic communication service or remote computing service or a communication common carrier shall disclose a record, the location information for а subscriber's or customer's mobile or wireless communications device, or other information pertaining to a subscriber or customer of the service, other than contents covered by subsections a. and f. of this section, to a law enforcement agency under the following circumstances:

(1) the law enforcement agency has obtained a warrant;

(2) the law enforcement agency has obtained the consent of the subscriber or customer to the disclosure;

(3) the law enforcement agency has obtained a court order for such disclosure under subsection e. of this section; or

with respect to only the location (4) information for a subscriber's or customer's mobile or wireless communications device and not to a record or other subscriber or customer information, the law enforcement good faith that agency believes in an emergency involving danger of death or serious bodily injury to the subscriber or customer requires disclosure without delay of information relating to the emergency. A law enforcement agency receiving records or information pursuant to this subsection is not required to provide notice to the customer or subscriber.

* * *

e. A court order for disclosure under subsection b. or c. may be issued by a judge

of competent jurisdiction and shall issue only if the law enforcement agency offers specific and articulable facts showing that there are reasonable grounds to believe that the record pertaining other information or to а subscriber or customer of an electronic communication service or remote computing service or communication common carrier is relevant and material to an ongoing criminal investigation. A judge who has issued an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

[(emphasis added).]

Disclosure of cell phone location information² is thus limited. Therefore, under the New Jersey Wiretap Act, a warrant or other judicial order is required for disclosure of the information at issue here to law enforcement.

Federal law similarly limits law enforcement access to cell phone location information. When Congress passed the Wireless Communication and Public Safety Act of 1999, for the purpose of facilitating deployment of enhanced 9-1-1 technology, privacy protection was specifically included for cell phone location information:

> (f) **Authority to Use Location Information.** For purposes of subsection(c)(1) of this

² "Location information" is defined in the New Jersey Wiretap Act as "global positioning system data, enhanced 9-1-1 data, cellular site information, and any other information that would assist a law enforcement agency in tracking the physical location of a cellular telephone or wireless mobile device." N.J.S.A. 2A:156A-2w.

section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to -

(1) Cell location information concerning the use of the commercial mobile service ...

[47 U.S.C. §222(f).]

The Communications Assistance for Law Enforcement Act, passed in 1994, mandated that court orders for pen register and trap and trace devices shall not include "any information that may disclose the physical location of the subscriber." 47 U.S.C. §1002(a)(2)(B).

While courts are divided over whether federal law requires law enforcement agents to obtain a warrant for real-time cell phone tracking, it is clear that, at minimum, they must obtain a court order upon a showing that the information is relevant and material to an ongoing investigation. The bases for law enforcement requests are Title II of the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§2701-2711 (2010), commonly referred to as the Stored Communications Act (SCA), and the Pen Register/Trap Trace Statute, also part of the SCA. Under 18 U.S.C. §2703(c)(1), information may be disclosed upon a warrant, court order or consent. Under 18 U.S.C. §3121, a court order is sufficient on a relevancy standard. Some courts have refused disclosure of location information in the absence of a warrant.³ Others have permitted disclosure by court order under the SCA.

³ See *infra*, note 10.

Accordingly, there is debate whether any federal statute is authority for disclosure of cell phone location information. But it is undisputed that some type of judicial authorization is required under federal law. Cell phone location information is thus protected under federal law as well.⁴

2. Cell Phone Customer Agreements and Privacy Policies

Cell phone provider privacy policies also support an expectation of privacy in location information. Customer agreements incorporate the providers' privacy policies and confirm protections against disclosure of location information to law enforcement. For example, defendant's provider, T-Mobile, has a policy that requires legal process, or an emergency, for disclosure to law enforcement.⁵ Every privacy policy we examined requires judicial process;⁶ none permits disclosure simply upon law

⁵ T-Mobile Privacy Policy, located at http://www.t-mobile.com/ company/website/privacypolicy.aspx.

⁴ Indeed, those privacy protections are now the subject of additional, proposed legislation which would strengthen users' privacy interests in cell phone location information. Several pieces of proposed legislation pending in the 112th Congress would clarify and, in some instances, strengthen privacy for cell phone location information. The proposed Electronic Communications Privacy Act Amendments Act (S.1011) requires a warrant for disclosure of geolocation information. Likewise, the Geolocational Privacy and Surveillance Act (S.1212 and H.R. 2168) likewise includes a warrant requirement for disclosure of this information.

⁶ <u>See, e.g.</u>, Sprint Nextel Privacy Policy, located at http://www.sprint.com/legal/privacy.html; AT&T Privacy Policy,

enforcement request. Such disclosure would violate the New Jersey Wiretap Act, the SCA and, we submit, the New Jersey Constitution.

users' location information is a category of As data specifically understood even by the provider as private, privacy policies expressly prohibit its disclosure without the subscriber's authorization. Providers' treatment of "location-based services" (LBS) also reflects an expectation that a user's location is private. These applications, uniquely available to cell phone subscribers, use location tracking and permit sharing this information with others. For example, the popular application "foursquare" permits cell users to share their location with "friends" by "checking in" at a given location. Foursquare, http://foursquare.com/privacy; also Google See Latitude, http://google.com/mobile/latitude (application permitting cell users to share their location with friends and to "[c]ontrol who sees your location.")

Without exception, providers give users of LBS notice and choice about whether LBS and attendant disclosure of location are activated. In fact, CTIA, the wireless trade association, has published "Best Practices and Guidelines for LBS," which requires providers to give notice and get consent before disclosing users' location information. CTIA, http://www.ctia.org/business_resources

located at http://att.com/gen/privacy-policy?pid=2506; Verizon
Privacy Policy, located at http://www22.verizon.com/privacy.

/wic/index/AID/11300. "[P]hone location tracking services are offered as `social' tools allowing consumers to find (or to avoid) others who enroll in these services." Jones, 565 U.S. at _____ (Alito, J., concurring in judgment).

3. Constitutional Privacy Interest in Tracking Technology

The constitutional privacy interest in law enforcement tracking is well-established. In <u>United States v. Karo</u>, 468 U.S. 705 (1984), the Supreme Court held that location tracking implicates Fourth Amendment privacy interests because it may reveal information about individuals in areas where they have reasonable expectations of privacy. Using an electronic device to infer facts about the inside of a protected place is just as unreasonable as searching it without a warrant. <u>Id.</u> at 714-15; <u>see also Kyllo v.</u> <u>United States</u>, 533 U.S. 27, 36 (2001) (explaining thermal imaging of a home violates the Fourth Amendment). As in these cases, cell phone tracking differs from the beeper tracking approved in <u>United States v. Knotts</u>, 460 U.S. 276 (1983), which reveals only information visually observable on a public highway.

<u>Karo</u> compels the conclusion that cell phone tracking implicates constitutional privacy interests. On any given day, a person's cell phone travels through many protected locations, where, under <u>Karo</u>, police cannot warrantlessly intrude on individuals' reasonable expectations of privacy. 468 U.S. at 716; <u>see Kyllo</u>, 533 U.S. at 34 (reasonable privacy expectation in home);

<u>See v. City of Seattle</u>, 387 U.S. 541, 543 (1967) (business premises); <u>Stoner v. California</u>, 376 U.S. 483, 486 (1964) (hotel room).

Moreover, an individual's privacy interest in his location information is not limited to the home or other protected locations, because "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." <u>Katz v. United States</u>, 389 U.S. 347, 351 (1967). It is not merely the cell phone's location in each constitutionally protected space, but the sum of information gathered from surveillance of a person's movement, that "reveals an intimate picture of the subject's life that he expects no one to have short perhaps of his spouse," and that thus supports an expectation of privacy that society recognizes as reasonable. <u>United States v.</u> <u>Maynard</u>, 615 F.3d 544, 563 (D.C. Cir. 2010), <u>aff'd</u>, <u>Jones</u>, 565 U.S. _____ (2012); <u>Doe v. Poritz</u>, 142 N.J. at 89 (discussing compilation of otherwise scattered bits of information).

The Supreme Court recently addressed location tracking in <u>United States v. Jones</u>, 565 U.S. ____ (2012), but on such narrow grounds that it sheds little light here. The question presented was whether the physical attachment of a GPS device to a car and its subsequent use was a search under the Fourth Amendment. The majority resolved the case by concluding that, because attachment required a physical trespass, there was a Fourth Amendment search.

However, it reserved for another day the question of whether purely electronic surveillance - like the cell phone tracking in this case - violates an individual's reasonable expectation of privacy. In any event, this Court has routinely recognized that the New Jersey Constitution protects a more expansive vision of privacy than its federal counterpart. <u>Compare Hempele</u>, 120 N.J. at 215 (1990), <u>with</u> <u>California v. Greenwood</u>, 486 U.S. 35,37 (1988).

Tracking technology represents a serious threat to privacy interests. As the highest courts of several states and the District of Columbia Circuit have acknowledged, location monitoring can now be continuous and indiscriminate, and therefore represents a far greater invasion of privacy than beepers, which were monitored for the discrete purpose of ascertaining the destination of a particular object. See, e.q., Maynard, 615 F.3d at 555-59; State v. Campbell, 759 P. 2d 1040, 1048 (Or. 1988) (use of radio transmitter to locate defendant's vehicle was a search under the state constitution, and stating that "[a]ny device that enables police quickly to locate a person or object anywhere within a 40mile radius, day or night, over a period of days, is a significant limitation on freedom from scrutiny"); People v. Weaver, 909 N.E. 2d 1195, 1196-97 (N.Y. 2009) (warrantless use of GPS device violates state constitution); State v. Jackson, 76 P. 3d 212, 223-24 (Wash. 2003) (state constitution requires warrant for continuous GPS tracking surveillance for weeks).

Although one court described location information as "a proxy for [the suspect's] physical location" because the phone provides similar information to physical surveillance, <u>United States v.</u> Forest, 355 F.3d 942, 951 (6th Cir. 2004), <u>abroqated on other</u> <u>grounds</u>, <u>United States v. Booker</u>, 543 U.S. 220 (2005), that is an inapt analogy. A provider's disclosure of cell phone location information constitutes tracking without physical surveillance. Traditional surveillance would provide data about whether the phone is located in a constitutionally protected place. Cell phone

Consequently, cell phone tracking must be treated more restrictively than traditional surveillance. Cell phone tracking - including providers' disclosure of real-time and historical locations - moves beyond "naked-eye surveillance." <u>Kyllo</u>, 533 U.S. at 33, 35 n.2; <u>Maynard</u>, 615 F.3d at 565-66 (rejecting comparison of GPS monitoring to visual surveillance). Police access to cell phone location permits surveillance of a scope and magnitude not possible through visual surveillance, and without regard to constitutionally-protected spaces. Further, there is a potential for mass surveillance that previously would have been prohibitively expensive. <u>United States v. Garcia</u>, 474 F.3d 994, 998 (7th Cir. 2007).

In fact, restrictions on a provider's cell-site disclosure will not resolve the constitutional conundrum cell phone tracking

poses. That is because devices now exist that can track cell-phone location <u>without</u> the provider's knowledge or involvement. For example, police now can acquire cell users' location information directly through the use of "triggerfish," or "cell site simulators."⁷ Triggerfish are portable devices that mimic cell phone towers and trick cell phones into sending signaling information, which is then used to track the phone.⁸ Thus, unless courts reinforce constitutional limitations upon privacy intrusions, law enforcement may soon directly access users' phones into tracking devices without the users' and convert them knowledge or consent. See Note, William Curtis, Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes, 45 Columbia J.L. & Soc. Probs. 139 (Fall 2011) (discussing triggerfish technology as shifting the legal debate over cell phone tracking).

⁷ Julian Sanchez, FOIA Docs Show Feds Can Lojack Mobile Without Telco Help, ARS TECHNICA (Nov. 16, 2008), http://arstechnica.com/ tech-policy/news/2009/11/foia-doc-show-feds-can-lojack-mobileswithout-telco-help-ars.

⁸ U.S. Dept. of Justice, Electronic Surveillance Manual 38-40 (2005). There is no evidence "triggerfish" technology is widely available. In fact, the federal Government has deemed this information "Law Enforcement Sensitive," and has sought to withhold details about the technology. <u>See</u> 'Stingray' Phone Tracker Fuels Constitutional Clash, Sept. 22, 2011, found at http://online. wsj.com/article/SB10001424053111904194604576583112723197574.html.

C. Neither the Appellate Division Nor The State Correctly Gauges the Substantial Constitutional Threat to Privacy Cell Phone Tracking Poses.

1. The Appellate Division Decision.

The Appellate Division rejected defendant's constitutional challenge to warrantless acquisition of cell phone location information by police. It found no reasonable expectation of privacy in (1) the general location of a cell phone, or (2) movements on public highways. <u>State v. Earls</u>, 420 N.J. Super. 583, 599 (App. Div. 2011). The Appellate Division thereby implicitly rejected any privacy expectation in cell phone location information. The court declined to decide whether a "warrant would be required for the police to obtain cell phone information to determine the specific location of a suspect, particularly the suspect's location in a private place." <u>Id.</u>

The Appellate Division framed the issue incorrectly. By denying a privacy interest in a <u>cell phone's</u> location, the Appellate Division failed to recognize that the phone's location reveals the <u>user's</u> location. The court further failed to understand how cell tracking technology differs, and is far more invasive, than past "beeper" technology. The trial court, but not the Appellate Division, recognized how police use of one's cell phone to track movement poses a threat to privacy interests. 4T20-13.

The Appellate Division erroneously relied upon <u>Knotts</u>, 460 U.S. at 276, where police were permitted to place and track a beeper as it traveled a single route over public highways. <u>Earls</u>, 420 N.J. Super. at 595-99. As previously explained, cell phone location technology is different. Unlike in <u>Knotts</u>, and more as in <u>Karo and Kyllo</u>, cell phone location technology tracks individuals in ways that cannot be accomplished through visual surveillance. It also reveals location within protected areas. Cell phone location information exists for all locations and is not conditioned on the possibility that a defendant may have traveled over a public highway. The <u>Knotts</u> public movement exception to privacy is therefore inapposite.

The Appellate Division's other authorities, which rely on <u>Knotts</u>, <u>id</u>. at 597-99, are equally unpersuasive and should not guide this Court. In <u>United States v. Forest</u>, 355 F.3d 942, 950-52 (6th Cir. 2004), tracking was done solely on public highways, along with visual surveillance. In <u>Devega v. State</u>, 689 S.E. 2d 294, 300 (Ga. 2010), the Court wrongly found that cell phone location "revealed the same information as visual surveillance." (quoting <u>Stone v. State</u>, 941 A. 2d 1238, 1250 (Md. Ct. Spec. App. 2008)). Cell phone location is not a proxy for visually identifiable location in a public place. Were it otherwise, law enforcement would not need this information from the provider to track a suspect. Police would simply use visual surveillance.

No reason exists to accept the dubious premise that cell phone tracking information reveals only public information available through visual surveillance. Cell phone tracking technology does not respect boundaries of protected areas. Here defendant was located in a motel room, not on a public highway, when police tracked his cell phone with the provider's assistance.

That is why the Appellate Division's artificial distinction between the police conduct here and a hypothetical attempt "to determine the specific location of a suspect, particularly the suspect's location in a private place" was inapt. <u>Earls</u>, 420 N.J. Super. at 599. There is no such distinction. The police sought defendant's location, wherever he was to be found. As it turns out, he was not located in public.

The Appellate Division's analysis, equating cell phone location information with visual surveillance, is incorrect for another reason. When police seek historical location information, they may retrospectively obtain data for times when physical surveillance was never done or even contemplated. For example, were police investigating a months-old crime, historical location information could trace a suspect's movements around the time of the crime. Police would not have surveilled at the time because the crime had not yet occurred. Yet tracking technology permits such retroactive surveillance.

This is not merely an aid to physical surveillance. This investigative technique reveals information which could not have been surveilled in real time. One's movement information is recorded by the cell provider. This location information operates as a retroactive tracking device without the user's knowledge.

This Court should therefore reverse the Appellate Division and hold that individuals have a reasonable expectation of privacy in cell phone location information.

2. The State's Position

The State incorrectly argues defendant had no reasonable expectation of privacy in his cell phone location information. The State's arguments erroneously characterize the technological facts. From this faulty premise, the State additionally misapprehends the nature of the information disclosed as well as the privacy interests implicated.

First, the State wrongly frames the question of whether defendant has a privacy expectation in the "generalized location" of his cell phone "within the context of fully public areas." Pb16. The State asserts that "police merely obtained basic information concerning the recent vicinity of defendant's phone <u>within a mile radius</u> of a given cell tower." Pb16 (emphasis in original). From this, the State claims this is "little more than the enhancement of the surveillance" police might have conducted visually. Pb16.

Each of these assertions is wrong. The police sought defendant's actual location and did not seek to limit the accuracy of information T-Mobile provided. Police likewise did not set limits upon this disclosure to public areas. The police were tracking defendant and wanted to find him at any location. In fact, Defendant's phone was at the motel, not in public.

Moreover, T-Mobile's disclosure substituted for visual surveillance. It was not a mere enhancement. There is also no reason to accept that the provider's disclosure was somehow limited to a mile perimeter. The accuracy of cell-site data is approaching that of GPS and depends upon the population density of a given location area. Yet the State would have the Court accept the fiction that police were not seeking precise location data. They were.

Second, the State's reliance on the New Jersey Wiretap Act to deny a privacy expectation should be rejected. The State argues that the Act's emergency exception, permitting disclosure of subscriber location when the subscriber is in danger, somehow undermines privacy expectation. The opposite is true. As we note, *supra*, the Act's privacy protections establish and confirm an expectation of privacy. Even the newly-enacted emergency exception in the Act did <u>not</u> permit T-Mobile's disclosure to police because defendant was not in danger.

Third, the State's reliance upon the public movement doctrine is misplaced. Contrary to the State's argument, cell phone location is not merely a proxy for visually observable location. Pb20-25. Defendant's phone was not even located in public. The State's suggestion that T-Mobile's provision of "vague" information was somehow less revealing than visual surveillance, Pb25-26, ignores the reality that police used the information to track defendant whether or not he may have been in public.

Fourth, the State's purported reliance upon the emergency aid exception to the warrant requirement is meritless. The State has offered no explanation why a warrant for the cell-site data was not sought after issuance of the arrest warrant. Police plainly had the opportunity to secure a warrant for this information. If they truly feared for a witness's safety, they could have called the issuing Judge and sought a warrant for location information.

Equally significant is the fact that the strict requirements for the emergency aid exception are plainly not met. There is no evidence of imminent emergency. The police concededly were partly motivated by the desire to find evidence against defendant.

POINT II

LAW ENFORCEMENT ACQUISITION OF CELL PHONE LOCATION INFORMATION SHOULD REQUIRE A WARRANT SUPPORTED BY PROBABLE CAUSE AND PARTICULARITY.

Police used no judicial process to request defendant's cell phone location information from T-Mobile. That conduct, together with T-Mobile's provision of the information, violated the New Jersey Wiretap Act, the SCA, and T-Mobile's own Privacy Policy. That conduct, absent some prior judicial review and approval, violates the New Jersey Constitution.

This Court should require a warrant based upon probable cause before police may access this information. The New Jersey Wiretap Act requires issuance of a warrant or court order before location information is disclosed to law enforcement. N.J.S.A. 2A:156A-29. The warrant requirement, as set forth at <u>R.</u> 3:5-3, is the appropriate vehicle for obtaining cell phone location information. Courts have the authority to issue search warrants to search and seize any property or documents. <u>R.</u> 3:5-2.

Cell phone location surveillance is akin to law enforcement use of a tracking device. Many other states have concluded that tracking device information may only be disclosed through the warrant process.⁹

⁹ Several states have enacted legislation requiring the exclusion of evidence produced by electronic tracking devices unless obtained by the police acting pursuant to a warrant. <u>See, e.g.</u>, Utah Code Ann. §§77-23a-4, 77-23a-7, 77-23a-15.5; Minn Stat. §§626A.37, 626A.3.5; Fla. Stat. §§934.06, 934.42; S.C. Code Ann. §10-30-140;

Even if cell phone location is not likened to tracking devices, other factors require a warrant for disclosure. Location information can be revealing, much like the contents of a phone call or an electronic mail. Location information is more revealing than, say, ISP subscriber information, for which a grand jury subpoena is sufficient for disclosure. <u>Reid</u>, 194 N.J. at 390.

Because cell phone tracking can be as continuous and indiscriminate as eavesdropping, wiretapping or video surveillance, and because cell phone location information reveals substantive data about individuals' affairs, a warrant for this type of surveillance should mirror the requirements now in place for intercept orders. These requirements include: (1) certification that "normal investigative procedures" have failed or will likely fail; (2) "a particular description of the type of [information] sought ... and a statement of the particular offense to which it relates"; (3) a period of surveillance no longer than necessary, and (4) a minimzation requirement. <u>United States v. Torres</u>, 751 F. 2d 875, 883-84 (7th Cir. 1984) (adopting these four warrant requirements for video surveillance). <u>See also</u> N.J.S.A. 2A:156A-9(c) (New Jersey Wiretap Act requirements for intercept orders).

The warrant requirement will check unbridled surveillance by

Okla. Stat. Ct. 13, §§126-6; 177.6; Haw. Rev. Stat. §§ 803-42, 803-44.7; 18 Pa. Cons. Stat. §5761 (statutory references collected at <u>United States v. Maynard</u>, 615 F.3d at 564, <u>aff'd</u>, <u>Jones</u>, 565 U.S. _____ (2012), and holding that warrantless use of GPS device on defendant's vehicle was an unconstitutional search).

law enforcement. In the context of cell phone location information, a warrant requirement will limit access to individuals' locations, movement and associations. Absent that requirement, police could acquire intimate information without regard to need or other limiting factors, such as manner, duration and scope of surveillance. Put simply, police could monitor a cell user's movements continuously.

Law enforcement acquisition of cell phone location information should be circumscribed at least as strictly as other law enforcement searches and seizures. Location information is too sensitive for police to access it in criminal investigations without a warrant. That is why a court order, based solely upon relevancy, is insufficient protection. A grand jury subpoena, likewise, offers no real judicial limitation upon police acquisition of sensitive, content-based location information. The "relevancy" standard poses the additional concern that police could capture broad swaths of information, such as the location information for all callers to a target cell phone.

Federal courts are divided on whether a warrant is required for law enforcement access to cell phone location information. The issue arises during *ex parte* government applications to compel providers to disclose real-time or historical cell phone location information. Several federal courts have required a warrant for the

disclosure of cell phone location information.¹⁰ Those decisions hold that existing federal statutes do not permit disclosure. Other courts have not required a warrant supported by probable cause. Those courts permit disclosure under the SCA based upon court order. <u>See In re Application of the United States for an</u> <u>Order Relating to Target Phone 2</u>, 733 F. Supp. 2d 939, 941 n.1 (N.D. Ill. 2009) (collecting authorities).

The Third Circuit is the only Court of Appeals to consider the issue. 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).

Obviously, in this case, law enforcement obtained neither a warrant nor a court order.

¹⁰ See, e.g., <u>In re Application for the Installation and Use of</u> <u>a Pen Register</u>, 439 F. Supp. 2d 456, 457 (D. Md. 2006); <u>S.D. Texas</u> <u>Opinion</u>, 747 F. Supp. 2d at 845; <u>In re Application for Pen Register</u> <u>and Trap/Track Device with Cell Site Location Authority</u>, 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005); <u>In re Application of the United</u> <u>States for an Order Authorizing the Disclosure of Prospective Cell</u> <u>Site Information</u>, 412 F. Supp. 2d 947, 949 (E.D. Wis. 2006); <u>In re</u> <u>Application for Pen Register and Trap/Trace Device with Cell Site</u> <u>Location Authority</u>, 396 F. Supp. 2d 294, 295 (E.D.N.Y. 2005).

POINT III

SUPPRESSION IS THE PROPER REMEDY FOR LAW ENFORCEMENT'S IMPROPER ACQUISITION OF CELL PHONE LOCATION INFORMATION.

In this case, police acquisition of cell phone location information from the provider without a warrant or court order violated the New Jersey Wiretap Act, N.J.S.A. 2A:156A-29c, and the SCA, 18 U.S.C. §§2703(c)(1) and 3121, as well as the New Jersey Constitution. The exclusionary rule should therefore apply. <u>See</u> <u>Reid</u>, 194 N.J. at 405 (ISP subscriber information constitutionally protected); <u>compare with State v. Gadsden</u>, 303 N.J. Super. 491, 505 (App. Div.), <u>certif. denied</u>, 152 N.J. 187 (1997) (denying suppression where procedural violations are not of constitutional dimension).

The exclusionary rule "advances the 'imperative of judicial integrity' and removes the profit motive from 'lawless behavior.'" <u>State v. Badessa</u>, 185 N.J. 303, 311 (2005) (quoting Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 1.5(c) (3d ed. 1996 & Supp. 2003)); <u>Evers</u>, 175 N.J. at 376. The rule thereby deters police misconduct and encourages respect for protected rights. <u>Reid</u>, 194 N.J. at 405.

Existing statutory remedies do not adequately protect defendants whose cell phone location information is unlawfully acquired by law enforcement. The New Jersey Wiretap Act provides for civil and criminal remedies for specified violations. A motion to suppress may be filed to suppress the "contents" of any "intercepted wire, electronic or oral communication, or evidence derived therefrom." N.J.S.A. 2A:156A-21. This suppression remedy is limited to the <u>contents</u> of communications.

This suppression remedy does not exclude location information or derivative evidence obtained in violation of 2A:156A-29c. For such violations, the New Jersey Wiretap Act permits the filing of a civil action for appropriate relief, including equitable or declaratory relief, or money damages.¹¹

Like this Court held in <u>Reid</u>, in these circumstances "[t]he Wiretap Act does not provide an adequate remedy." <u>Reid</u>, 194 N.J. at 405. Simply put, statutory civil remedies cannot make defendant whole. Civil remedies are hollow. Self-incrimination concerns often prevent criminal defendants from pursuing civil claims during criminal proceedings. Civil actions are also costly and timeconsuming. Establishing damages is difficult if not impossible. Similarly, declaratory relief is likely to be transitory, if not illusory.

Prosecutors should not be permitted to "profit" from unlawful conduct by law enforcement. Otherwise New Jersey would have perverse incentive to disregard statutory rights if it decides that the evidence to be obtained is more valuable than possible civil penalties which may later be imposed for its acquisition. Criminal

¹¹ 2A:156A-24. As this Court has noted, the SCA fails to provide for a suppression remedy for a violation. <u>State v. Evers</u>, 175 N.J. 355, 374 (2003) (internal citation omitted).

defendants should not be required to seek relief solely through inadequate civil remedies while they suffer the State's use of unlawfully procured evidence to convict and to sentence them under our criminal laws.

Further, the interests of both deterrence and judicial integrity are served by the suppression of the unlawfully acquired evidence here. In the present case, the police used no judicial process to seize defendant's cell phone location information. Nevertheless, T-Mobile turned over the location information. Using this information, police tracked down defendant's vehicle and, directly from this discovery, located defendant in a motel room, where incriminating evidence was seized. The improperly-obtained location information immediately led to defendant's arrest and the seizure of additional, inculpatory evidence.

Only suppression of the unlawfully obtained evidence can achieve the goal of deterrence. Otherwise, law enforcement can act with impunity. Further, the use of the evidence here would offend the integrity of the judicial process. <u>Evers</u>, 175 N.J. at 380.

CONCLUSION

Police used unlawful means to acquire defendant's legally protected cell phone location information, by disregarding established standards for obtaining constitutionally (and statutorily) protected information held by the cell phone provider. Their warrantless acquisition of this information violated the New Jersey Constitution, and illustrates the grave dangers to individual privacy and freedom of association posed by recent developments in cell phone location technology.

Accordingly, for the foregoing reasons, amici respectfully urge the Court to reverse the Appellate Division by: (1) recognizing the constitutional right to privacy, under Article I, paragraph 7 of the New Jersey Constitution, for cell phone location information; (2) requiring a warrant, supported by probable cause and particularity, before law enforcement acquires this location information; and (3) granting the suppression remedy for law enforcement's unlawful acquisition of cell phone location information.

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: