SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK, PART 62
----------X

PEOPLE OF THE STATE OF NEW YORK,

- against - **Indictment No. 5652/2014**

ALI MOALAWI*, et ano*.,

Defendants.

----------X

THE DEFENDANT ALI MOALAWI'S MEMORANDUM OF LAW IN SUPPORT OF HIS MOTION TO SUPPRESS THE PEOPLE'S CSLI EVIDENCE ON THE GROUNDS THAT THE SEIZURE, ACQUISITION AND MAINTENANCE OF 201 DAYS OF THE DEFENDANT'S CSLI DATA WAS A VIOLATION OF HIS CONSTITUTIONAL RIGHTS GUARANTEED BY THE CONSTITUTIONS OF THE UNITED STATES AND THE STATE OF NEW YORK

Law Office of
JOHN W. MITCHELL
P.O. Box 163
Bedford, New York 10506

Table of Contents

History and Travel of This Case…….. 1

Survey of the Case Law Relevant To the Instant Motion to Suppress……. 4

Olmstead and *Katz*…….. 4

The Third Party Disclosure Doctrine and/or
Assumption Of the Risk Cases: *Miller* and *Smith*……... 6

The Beeper cases: *Knotts, Karo* and *Kyllo*…….. 8

The Decisions by the Supreme Court in
United States v. Jones and *Riley v. California*……. 11

Riley v. California……... 19

Relevant State Court Decisions…….. 20

The Decisions by the New York State Court of Appeals in
People v. Weaver and *Matter of Cunningham v New York State Dept. of Labor*……. 26

Other New York Decisions Which
Relate to the Issues Before the Court…….. 30

Technological Advances Continue to Require the
Evolution and Recalibration of Fourth Amendment Doctrine…… 35

This Court Should Apply Mosaic Theory to Resolve Whether The Acquisition
Of Defendant's Historical CSLI Data was a "Search" Within the Meaning
Of The 4th Amendment and/or Art. 1, § 12 of the N.Y. Constitution……... 37

In *People v. Weaver* and *Matter of Cunningham v. New York State
Dept. of Labor*, the Court of Appeals Applied Mosaic Theory to
Resolve the "Reasonable Expectation of Privacy" Test of *Katz*…….. 39

This Court Should Apply Mosaic Theory to Determine
The Instant Motion to Suppress…….. 40

Application of the Third Party Disclosure
And/Or Assumption of Risk Doctrines……... 49

The D-Order, Which Required the Production of the Defendant's CSLI for a
Period of Six & ½ Months Was, In Effect, the Equivalent of a "General Warrant"……. 52

The First Amendment Has Also Been Violated
By The Prolonged Location Tracking of Mr. Moalawi……... 56

The Historical CSLI Should Be Suppressed Because the
Defendant's Phone Was Monitored From Locations in
Which He had a Traditionally Recognized Expectation of Privacy……. 58

It Is The Duty Of This Court To Resolve
The Constitutional Case and Controversy Presently Before It…… 59

This Court Should Grant the Defendant's Motion to Suppress……... 63

Conclusion…….. 64

Table of Authorities

Cases:

ACLU v. Clapper,
2015 U.S. App. LEXIS 7531(2d 2015)……... 56

Commonwealth v. Augustine,
467 Mass. 230, 4 N.E.3d 846 (2014)…….. 21

Commonwealth v. Pitt,
29 Mass. L. Rep. 445, 2012 Mass. Super. LEXIS 39 (Mass. Super. Ct. 2012)…….. 34

Commonwealth v. Wyatt,
30 Mass. L. Rep. 270, 2012 Mass. Super. LEXIS 248 (Mass. Super. Ct. 2012)…… 25

Davis v United States,
___U.S. ___, 131 S Ct 2419, 180 L. Ed. 2d 285 (2011)……... 33

In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011)…….. 43

In re U.S. for an Order Authorizing the Release of historical Cell-Site Info.,
809 F. Supp. 2d 113 (E.D.N.Y. 2011)……. 43, 45

In re Application of US for Order Directing Provider of Elec. Communication Serv. to Disclose Records to Govt., 620 F3d 304 (3d Cir. 2010)……. passim

In re Cellular Tels.,
2014 U.S. Dist. LEXIS 182165 (D. Kan. 2014)……. 36

In re Smartphone Geolocation Data Application,
977 F.Sup.2d 129 (E.D.N.Y. 2013)……. 43

In re United States,
20 F. Supp. 3d 67 (D.D.C. 2013)…….. 3

Katz v. United States,
389 U.S. 347, 88 S. Ct. 507 (1967)……. passim

Klayman v. Obama,
957 F. Supp. 2d 1 (D.D.C. 2013)…… 45

Kyllo v. United States,
533 U.S. 27, 121 S. Ct. 2038 (2001)……... 10, 11

Matter of Cunningham v. New York State Dept. of Labor,
21 N.Y.3d 515, 974 N.Y.S.2d 896 (2013)…….. passim

NAACP v. State of Ala. ex rel. Patterson,
357 U.S. 449, 78 S. Ct. 1163 (1958)…….. 57

Olmstead v. United States,
277 U.S. 438, 48 S. Ct. 564 (1928)……. passim

People Bigelow,
66 N.Y.2d 417,.497 N.Y.S.2d 630 (1985)…….. 34

People v. Hall, 86 A.D. 3d 450,
926 N.Y.S. 2d 514 (1st Dep't. 2011)…….. 30, 41

People v. Moorer, 39 Misc. 3d 603,
959 N.Y.S.2d 868 (County Ct., Monroe Ct. 2013)……. 33, 42

People v. Watkins,
125 A.D.3d 1364, 2015 N.Y. App. Div. LEXIS 1102 (4th Dep't. 2015)……... 32, 41

People v Wells,
45 Misc. 3d 793, 991 N.Y.S.2d 743 (Sup. Ct. Queens Cty. 2014)……. 35

People v. Weaver,
52 A.D.3d 138, 860 N.Y.S.2d 223 (3d Dep't. 2008)…….. 26

People v. Weaver,
12 N.Y.3d 433, 882 N.Y.S.2d 357 (2009)…….. passim

Riley v. California,
___ U.S. ___, 134 S. Ct. 2473 (2014)……. passim

Smith v. Maryland,
442 U.S. 735, 99 S. Ct. 2577 (1979)……... passim

State v. Earls,
214 N.J. 564, 70 A.3d 630 (2013)……... 20

Tracy v. Florida,
152 So. 3d 504, 2014 Fla. LEXIS 3072 (2014)…….. 25, 51

United States v. Cooper,
2015 U.S. Dist. LEXIS 25935 (N.D. Cal. 2015)…… 43, 63

United States v. Davis,
754 F.3d 1205 (11 Cir. 2014)…….. 44

United States v. Davis,
2015 U.S. App. LEXIS 7385 (11th Cir. 2015)…… passim

United States v. Jones,
451 F. Supp. 2d 71 (D.C.D.C. 2006)……... 10

United States v. Jones,
565 U.S. ___, 132 S. Ct. 945 (2012)…….. passim

United States v. Katzin,
732 F.3d 187 (3d Cir. 2013)…… 39

United States v. Karo,
468 U.S. 705, 104 S. Ct. 3296 (1984)……. passim

United States v. Knotts,
460 U.S. 276, 103 S. Ct. 1081 (1983)……. passim

United States v. Maynard,
615 F.3d 544 (D.C. Cir. 2010)…… passim

United States v. Miller,
425 U.S. 435, 96 S. Ct. 1619 (1976)……... passim

United States v. Powell,
943 F. Supp. 2d 759 (E.D. Mich. 2013)…….. 43

United States v. Shah,
2015 U.S. Dist. LEXIS 826 (E.D.N.C. 2015)……. 44

United States v. Skinner,
690 F.3d 772 (6th Cir. 2012)…… 42

United States v. White,
2014 U.S. Dist. LEXIS 166444 (E.D. Mich. 2014)…… 40, 53

Constitutional Provisions:

United States Constitution, First Amendment…… passim

United States Constitution, Fourth Amendment……. passim

United States Constitution, Fourteenth Amendment…….. 63, 64

New York Constitution, Article 1, § 12…….. passim

Massachusetts Declaration of Rights, Art. 14……. 21

New Jersey Constitution, Article I, Paragraph 7……. 20

Laws and Rules

Stored Communications Act,
18 U.S.C. § 2703(d)……..……. passim

New York Civil Rights Law, Section 8…….. passim

New York Criminal Procedure Law, § 460.20 (2)(a)……. 27

Colo. Rev. Stat. Ann. § 16-3-303.5(2)…… 47

16 Me. Rev. Stat. § 648……... 47

Mont. Code Ann. § 46-5-110(1)(a)……. 47

Utah Code Ann. § 77-23c-102(1)(a)……... 47

Learned Treatises:

Alexander Galicki, *The End Of Smith V. Maryland?: The NSA's Bulk Telephony Metadata Program And The Fourth Amendment In The Cyber Age*, 52 Am. Crim. L. Rev. 375 (2015)……... 45

Andrew Crocker, *Trackers That Make Phone Calls: Considering First Amendment Protection For Location Data*, 26 Harv. J. Law & Tec 619 (2013)……... 57

Brad Leneis, *Mapping A Way Out: Protecting Cellphone Location Information Without Starting Over On The Fourth Amendment*, 50 Am. Crim. L. Rev. 499 (2014)…….. 50

Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond The Content/Non-Content Distinction*, 54 Santa Clara L. Rev. 821 (2014)…… 19

Colleen Maher Ernst, *Looking Back to Look Forward: Reexamining the Application of the Third-Party Doc-Trine to Conveyed Papers*, 37 Harv. J.L. & Pub. Pol'y 329 (2014)…….. 49

Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112 (2007)……... 57

Hon. Stephen Wm. Smith, *Standing Up for Mr. Nesbitt*, 47 U.S.F. L. REV. 257 (2012) http://lawblog.usfca.edu/lawreview/wp-content/uploads/2014/09/Standing-Up-for-Mr.-Nesbitt.pdf..... 62

Katherine J. Strandburg, *Freedom Of Association In A Networked World: First Amendment Regulation Of Relational Surveillance*, 49 B.C. L. Rev 741 (2008)…….... 57

Miriam H. Baer, *Secrecy, Intimacy, and Workable Rules: Justice Sotomayor Stakes Out the Middle Ground in United States v. Jones*, 123 Yale L.J. F. 393 (2014)…… 36

Lauren E. Babst, *No More Shortcuts: Protect Cell Site Location Data With A Warrant Requirement*, 21 Mich. Telecomm. Tech. L. Rev. 363 (2015)……. 48

Orin Kerr and Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?* ABA Journal, August 1, 2012, http://www.abajournal.com/magazine/article/ the_data_question_should_the_third-party_records_doctrine_be_revisited/……..... 49

Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012)…….. 39, 41

Steven M. Bellovin, *When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J.L. & Liberty 556 (2014)……. 37, 38

Other Authorities:

Beyond the Beltway, Benenson Strategy Group, 2015, http://na-aba.marketo.com/rs/benensonstrategygroup/images/Beyond%20the%20Beltway%20February%202015%20 for%20Public%20Release%5B1%5D.pdf…… 47

Ken Strutin, *Mosaic Theory: A New Perspective for Human Privacy*, (NYLJ 9/24/13)……... 39

MSNBC, *Should Police Need A Warrant To Track Cell Phone Location Data?* http://www.msnbc.com/msnbc/poll-should-police-need-warrant-track-cell-phone-location-data..... 46

Obergefell v. Hodges, 14-556, Transcript of Oral Argument, April 28, 2015 http://www.supremecourt.gov/oral_arguments/argument_transcripts/14-556q1_6k47.pdf..... 60

Pew Research Ctr, What Americans Think About NSA Surveillance, National Security And Privacy, May 29, 2015 http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/..... 46

Update: Polls Continue to Show Majority of Americans Against NSA Spying, January 22, 2014, https://www.eff.org/deeplinks/2013/10/polls-continue-show-majority-americans-against-nsa-spying..... 47

United States v. Jones, No. 10-1259, Transcript of Oral Argument, at pp. 57-58, November 8, 2011 available at: http://www.supremecourt.gov/oral_arguments/argument transcripts/10-1259.pdf…… 48, 56

Legislative History:

H.R. Rep. No. 103-827, pt. 1 at 31 (1994)…… 44

Senate Report No. 103-402, at 31 (1994)……. 44

History and Travel of This Case

On September 17, 2014, the District Attorney's Office for New York County ("DANY"), acting pursuant to the federal Stored Communications Act (18 U.S.C. §7203[d]), submitted an Affirmation In Support of Application for Cell Site Order ("Application") to this Court.[1]

In that application, the People represented that based upon several snippets of CCTV footage that had been obtained in the course of an investigation by the New York City Police Department, as well as some DNA evidence that had been collected at two burglary sites, they suspected that an individual by the name of Ricky Moore had carried out a series of burglaries in midtown and lower Manhattan during the period from March 14, 2014 to September 17, 2014. The Application went on to explain that Ricky Moore had been previously convicted (and sentenced *in absentia*) for burglary in March of 2011, but that Mr. Moore had fled while the jury was in deliberation and that he had been a fugitive ever since.

Based upon the People's Application, this Court issued an Order pursuant to 18 U.S.C. §2703(d) (hereinafter the "D-Order") authorizing the acquisition of the Defendant, Ali Moalawi's, Cell Site Location Information ("CSLI") for a period of 6½ months (201 days) from March 1, 2014 to September 17, 2014.

The record further shows however, that instead of serving the wireless carrier (Sprint) with the D-Order that had been signed by the Court, instead, Sprint was served with a so-ordered grand jury subpoena.[2] It does not appear that the D-Order was ever served upon or even shown to Sprint since – at the request of the People – the Court directed that the D-Order be sealed.

[1] See, Affirmation In Support of Application for Cell Site Order, dated September 17, 2014 (Attached to the Affirmation of John W. Mitchell as Exhibit E thereto).

[2] Grand Jury subpoena attached to the Affirmation of John W. Mitchell at Exhibit G).

Furthermore, although the application for the D-Order was made by Assistant District Attorney Chloe Jones, the D-Order that was subsequently issued stated that it was based upon the showing made in the "application made by Assistant District Attorney Andrew Searle."[3]

As the factual presentation made by the People in support of the D-Order shows, they had little information to support their request for long term CSLI data of the Defendant. Most of the facts contained in the Application concerned information that the police had gathered with respect to Ricky Moore. In fact, all that the police could offer in their attempt to try and connect Mr. Moalawi to any burglary, was that on one occasion (March 14, 2014) they reviewed a CCTV video clip that appeared to show the "perpetrator [Ricky Moore] being assisted in leaving the location by a blue Volkswagen Jetta station wagon." And on a second occasion (July 28, 2014) the police represented that examining "surveillance video from the building adjacent to the crime scene and that on the video, [they] observed the same blue Volkswagen Jetta station wagon assisting the perpetrator of the crime in loading items into the trunk of the car before leaving the location."[4] The police subsequently learned that the car had been leased by Mr. Moalawi's employer (Carl Zeiss Microscopy, LLC) and had been given to Mr. Moalawi to be used for business activities and/or by himself or his wife for personal use.

Under § 2703(d), the government must "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." To satisfy this standard, the government must provide a sufficient factual basis to

[3] Order attached to Affirmation of John W. Mitchell, as Exhibit F.

[4] The video taken on July 28, 2014, and provided to the Defendant in discovery, is in black and white. It is not possible to tell the color of the car or to read its license plate.

the Court to justify its application ("specific and articulable facts"), and it must show that the data requested is relevant and material to the investigation." *In re United States*, 20 F. Supp. 3d 67, 72 (D.D.C. 2013).

Bearing this standard in mind, in assessing the sufficiency of the showing made in the Application, several relevant observations obtain. First, the police did not know who was operating the "blue Volkswagen Jetta station wagon" on March 14th and July 28th 2014. And it bears mention, that conspicuous by its absence, is any claim that Mr. Moalawi was identified in any of the CCTV footage that had been obtained by the police. Second, there are no allegations that Mr. Moalawi ever entered any building or residence, nor was any of Mr. Moalawi's DNA ever found at any alleged burglary site. Third, although the People relate that they were told by police officers that they suspected that Ricky Moore may have been involved in a series of burglaries, other than the conjecture of the police, the Application does not proffer any factual basis - or even circumstantial evidence – to support any finding that Mr. Moalawi had any connection, participation or knowledge of any of these other alleged burglaries. Fourth, and perhaps most significantly, in the Application the People expressly concede that at that time they petitioned this Court to issue the D-Order, they did not know whether Mr. Moalawi had been involved in these burglaries – indeed, as the Application states: "Cell site information will enable us to determine the general vicinity from where the target cell phone is transmitting, *so that we may determine whether Ali Moalawi was assisting Ricky Moore in committing the aforementioned burglaries*." (emphasis supplied) Finally, the fact that his car was seen on two occasions picking another person up is entirely consistent with lawful, innocent activity.

It is respectfully asserted that given the defects that exist with respect to the Application and D-Order, and to the process that was utilized to obtain the Defendant's records from Sprint

(i.e. that the actual D-Order was never shown to or served upon Sprint), that the Defendant's rights guaranteed by the First, Fourth and Fourteenth Amendments to the United States Constitution, Article 1, Section 12 of the Constitution of the State of New York and Section 8 of the New York Civil Rights Law have been violated, and that 18 U.S.C. § 2703 (d) is unconstitutional as applied. In this regard, the Defendant at bar does not argue that simply because the procedures revealed in this case may have constituted violations of the Store Communications Act, that suppression is warranted. Rather the Defendant's position is that suppression is warranted because his constitutional rights, guaranteed by both the United States Constitution and the Constitution of the State of New York were violated.

Survey of the Case Law Relevant
To the Instant Motion to Suppress

Olmstead* and *Katz

Undoubtedly the logical starting point in analyzing the evolution of the state and federal jurisprudence that applies to consideration and resolution of the issues presented at bar, is the Supreme Court's decision in *Olmstead v. United States*, 277 U.S. 438, 48 S. Ct. 564 (1928).

Mr. Olmstead was convicted of conspiring to violate the National Prohibition Act based upon evidence gathered when federal law enforcement officials wiretapped the telephone lines outside of Mr. Olmstead's offices. In the course of installing their wiretapping equipment, the law enforcement officers never directly trespassed upon any property belonging to Mr. Olmstead (they were able to tap his phones by accessing the public telephone lines). Following a review of the Court's Fourth Amendment decisions up to that point - in a 5 to 4 decision written by Chief Judge Taft - the Court held that no Fourth Amendment violation had occurred because "there was no entry of the houses or offices of the defendants." *Id.* at 464. The *Olmstead* Court maintained its fidelity to the premise that violations of the Fourth Amendment required a trespassory element,

and - "unless there has been an official search and seizure of [a] person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure" - no claim for a constitutional violation would lie. *Id.* at 568.

Justices Holmes, Brandeis, Butler and Stone dissented. In his dissenting opinion, Justice Brandeis urged the Court to recognize that as technological invention advanced the ways and means by which the government might seek to invade the privacy of the citizenry would predictably become more sophisticated. He admonished the Court that it had to recognize that unflagging reliance upon trespassory doctrine would be inadequate to protect against technological advances and the use of devices that would not need to be installed in the person's home or on property in which he had a traditionally recognized expectation of privacy. As Mr. Justice Brandeis exhorted: [C]onstitutions… are not ephemeral enactments, designed to meet passing occasions. They are, to use the words of Chief Justice Marshall 'designed to approach immortality as nearly as human institutions can approach it… [i]n the application of a constitution, therefore, our contemplation cannot be only of what has been but of what may be… [b]ut 'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." *Id*. at 473.

Justice Brandeis' admonishments notwithstanding, it would not be until 1967 when the Court decided *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507 (1967), that the arguments that he presented in his dissent in *Olmstead,* would be finally embraced.

Katz, like *Olmstead,* presented a case where there was no trespassory dimension, the police had attached a listening device to the outside of the phone booth from which Mr. Katz made his

bookmaking calls. No physical invasion of *Katz's* property had taken place. In analyzing whether a Fourth Amendment violation had occurred, the Court finally rejected the notion that the physical intrusion standard applied in *Olmstead* was the only determining criteria. In the now famous words of Mr. Justice Stewart: "[T]the Fourth Amendment protects people, not places." *Id.* at 351. Adopting this interpretation and application of the Fourth Amendment, the Court - no longer constrained to view the facts from the single prospective of trespassory theory - resolved the case by looking instead to "objective and evolving privacy expectations." Justice Harlan, in his concurring opinion, formulated the test for determining when the protections of the Fourth Amendment would engage - as he explained: "My understanding of the rule that has emerged… is that there is a twofold requirement, first that a person have exhibited an actual [subjective] expectation of privacy and, second, that the expectation be one that society is [objectively] prepared to recognize as 'reasonable.'" *Id.* at 361. Thus a person's right to be protected from an unreasonable search and seizure exists so long as the action being performed was something intended to be private, and that society would consider this expectation of privacy to be reasonable.

The Third Party Disclosure Doctrine and/or
Assumption Of the Risk Cases: *Miller* and *Smith*

The facts in *United States v. Miller*, 425 U.S. 435, 96 S. Ct. 1619 (1976), show that Mr. Miller was suspected of operating a "still" and running boot-leg moonshine without paying the government its "Whiskey Tax." Law enforcement agents issued a subpoena to the banking institutions where Mr. Miller did his banking business, demanding that the banks: "produce all records of accounts, i.e., savings, checking, loan or otherwise, in the name of Mr. Mitch Miller." *Id*. at 437. The banks provided the government with all of the subpoenaed records and did not inform Mr. Miller that it had done so. Mr. Miller's counsel made a pre-trial motion to suppress on the grounds, *inter alia*, that: "by requiring a third party bank to copy all of its depositors' personal

checks and then, with an improper invocation of legal process, [and by] calling upon the bank to allow inspection and reproduction of those copies," Miller's rights guaranteed by the Fourth Amendment prohibition against "unreasonable searches and seizures," had been violated. *Id.* at 439.

Miller's counsel argued that his client had a reasonable expectation of privacy in his bank records because he only made them available to his bankers for a limited purpose. However quoting its statement in *Katz* that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection," the Court reasoned that Miller's checks, financial statements, and deposit slips constituted information that Miller had "voluntarily conveyed" to the banks and their employees, and that one who reveals his affairs to another takes the risk that the other will convey that information to the government. Finding that the defendant therefore had no privacy interest in these records, the Court held that the Fourth Amendment had not been violated, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 442.

Mr. Justice Brennan, dissenting, arguing that the mere fact that the defendant allowed a third party to be in possession of his records, did not diminish his expectation of privacy for purposes of Fourth Amendment analysis. As Justice Brennan wrote: "[T]he disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account… [t]o permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power." *Id.* at 451

Three years later, in *Smith v. Maryland*, 442 U.S. 735, 99 S. Ct. 2577 (1979), the Supreme Court held that the installation and use of a pen register on a defendant's telephone to record the numbers he dialed - without first obtaining a warrant - did not constitute a search under the Fourth Amendment. Adopting the *Miller* analysis, the Court found that the defendant's use of the telephone company's services, and the resulting exposure of that information to the phone company and its employees, demonstrated that he "assumed the risk" that the telephone company or its employees would disclose the numbers he dialed to the police. To wit: "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744.

The Beeper cases: *Knotts, Karo* and *Kyllo*

In 1983 the Court decided *United States v. Knotts*, 460 U.S. 276, 103 S. Ct. 1081 (1983). In *Knotts*, law enforcement agents placed a beeper tracking device inside a container of chloroform which they suspected was being purchased to manufacture illegal drugs. The beeper emitted a periodic signal which agents monitored with a radio receiver. When a codefendant purchased the chloroform, the officers followed the car in which the container had been placed. Through the combination of visual surveillance and tracking the radio beacon, the police were able to trace the container to the location of the defendant's cabin. Based upon that information, the police applied for a warrant to search the cabin.

Defense counsel moved to suppress the evidence obtained from the cabin. The district court denied the motion but the Eighth Circuit reversed on appeal. Certiorari was granted and the Supreme Court ultimately held that no Fourth Amendment violation had occurred. The Court

reasoned that: "[G]overnmental surveillance conducted by means of the beeper amounted principally to the following of an automobile on public streets, there being no expectation of privacy in having a car observed arriving on one's premises after leaving a public highway, and since the scientific enhancement of the beeper raised no constitutional issues that visual surveillance would not also raise." *Id.* at 285.

However the Court went on to note that the "Respondent does not actually quarrel with this analysis, though he expresses the generalized view that the result of the holding sought by the Government would be that 'twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision… [b]ut the fact is that the 'reality hardly suggests abuse'… *if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable*." *Id.* at 283 (emphasis supplied).

One year after *Knotts*, the Supreme Court was once again called upon to decide a case involving the use of beeper tracking technology. In *United States v. Karo*, 468 U.S. 705, 104 S. Ct. 3296 (1984), DEA agents learned that the defendant had ordered 50 gallons of ether from a government informant. They obtained a court order authorizing the installation and monitoring of a beeper in one of the cans of ether. By monitoring the beeper, the agents eventually tracked the ether to the defendants' residence.

Distinguishing the circumstances presented in *Knotts* from those in *Karo*, the Court observed that: "In *Knotts*, the record did not show that the beeper was monitored while the can containing it was inside the cabin, and we therefore had no occasion to consider whether a constitutional violation would have occurred had the fact been otherwise." *Id.* at 714. "This case thus presents the question whether the monitoring of a beeper in a private residence, a location not

open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." *Id.* at 714.

The Court emphasized that this was not an instance in which the information supplied by the beeper was nothing more than that which could otherwise have been "conveyed to anyone who wanted to look…" because in *Karo*, "the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified." *Id.* at 715. Thus, while the Court had held in *Knotts* that it was it was permissible to electronically track an individual on public roadways where there was purportedly no expectation of privacy - once that individual reached his home - the electronic device could not be used "to obtain information that [the Government] could not have obtained by observation from outside the curtilage of the house." *Id.* at 715.

Seventeen years later, in 2001, the Court decided *Kyllo v. United States,* 533 U.S. 27, 121 S. Ct. 2038 (2001). In that case, law enforcement personnel used a thermal imaging device to scan the defendant's home to determine whether the amount of heat radiating from the house was consistent with use of the high-intensity lamps typically required for growing marijuana indoors. The information obtained from the thermal imaging was then used to apply for a search warrant for the home.

The Court began by noting that: "We have previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much…. [t]he question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Id*. at 33-34.

Applying the *Katz* protocol, the Court analyzed the facts through the dual lenses of subjective and objective expectations of privacy. To wit: " [A]s Justice Harlan's oft-quoted concurrence described it, a Fourth Amendment search occurs when the government violates a

subjective expectation of privacy that society recognizes as reasonable… [w]e have subsequently applied this principle to hold that a Fourth Amendment search does not occur - even when the explicitly protected location of a house is concerned - unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society [is] willing to recognize that expectation as reasonable.'" *Id*. at 33.

The Court concluded that heat imaging of the suspect's home constituted a search under the Fourth Amendment and required a search warrant. Relying on the reasoning of *Karo*, the Court found that because information that emanated from inside of the defendant's home had been obtained, a Fourth Amendment violation had occurred because an "intrusion into a constitutionally protected area" had taken place. And, while the Court acknowledged the government's contention that the thermal imaging equipment used in *Kyllo* was "crude," the Court explained that: "The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained." *Id*. at 37. As Mr. Justice Scalia concluded: "We have said that the Fourth Amendment draws 'a firm line at the entrance to the house,' *Payton*, 445 U.S. at 590. That line, we think, must be not only firm but also bright - which requires clear specification of those methods of surveillance that require a warrant." *Id*. at 40. The Court went on to emphasize that "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." *Id.* at 35-36.

The Decisions by the Supreme Court in *United States v. Jones* and *Riley v. California*

The history and travel of the events in *United States v. Jones*, 565 U.S. ___, 132 S. Ct. 945 (2012) show that Jones was a nightclub owner in the District of Columbia. He was suspected by law enforcement of dealing drugs. While Jones's wife's Jeep was parked in a public parking lot,

law enforcement agents surreptitiously installed a GPS tracking device. Without benefit of a warrant, the agents monitored Mr. Jones' movement 24 hours a day for a period of 4 weeks. In the district Court (*United States v. Jones*, 451 F. Supp. 2d 71 [D.D.C. 2006]), Jones' counsel moved unsuccessfully to suppress the data obtained from the mobile tracking device. 451 F. Supp. 2d at 87-88. Based, in part, upon thousands of pages of location information gathered from the device over the period of surveillance, Jones was convicted of a drug trafficking conspiracy and sentenced to life imprisonment.

The District Court resolved the matter by applying the reasoning in *Knotts* and *Kayo.* Applying *Knotts*, the Court held that Jones did not have any expectation of privacy when the Jeep was being tracked on the public thoroughfares – to wit: "[N]o Fourth Amendment violation through installation of GPS device without a warrant because 'law enforcement personnel could have conducted a visual surveillance of the vehicle as it traveled on the public highways.'" *Id.* at 88. Applying *Kayo*, the Court held that any data obtained during the periods that the Jeep was parked at Jones residence had to be suppressed – to wit: "[A]s the government here essentially concedes… the data obtained from the GPS device when the Jeep Cherokee was parked in the garage adjoining the Moore Street property must be suppressed." *Id.* at 88.

Following his conviction, Jones appealed to the D.C. Court of Appeals (the case was captioned *United States v. Maynard*, 615 F.3d 544 [D.C. Cir. 2010]). The defense argued that through the use of GPS tracking technology and the ability to see the data points in the aggregate, the invasion of privacy that occurred was substantively different than merely following a suspect on a common thoroughfare. The government argued that it was immaterial whether it had electronically tracked Jones for two days or two months, because in the Government's view,

United States v. Knotts controlled and Jones had no reasonable expectation of privacy in his movements on public streets. *Id.* at 615 F.3d at 556-557.

Circuit Judge Douglas Ginsburg, writing for a unanimous court, pointed out that the Supreme Court in *Knotts* expressly reserved the question of whether a different result would have obtained if the nature of the surveillance that had occurred in that case had been constant and for an extended period of time. As Judge Ginsburg noted: "Most important for the present case, the Court [in *Knotts*] specifically reserved the question of whether a warrant would be required in a case involving 'twenty-four hour surveillance,' stating if such dragnet-type[5] law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id*. at 556.

Distinguishing the facts in *Knotts* from those presented in *Jones*, the Court explained: "Here the police used the GPS device not to track Jones's 'movements from one place to another,' *Knotts*, 460 U.S. at 281, but rather to track Jones's movements 24 hours a day for 28 days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place to place." *Id.* at 615 F.3d at 558.

The Court then turned to the first prong of the *Katz* test to determine whether Jones – subjectively - had a reasonable expectation of privacy in his movements. The Court held that he did: "Two considerations persuade us the information the police discovered in this case - the

[5] The Court in *Maynard* also addressed the Government's contention that the reference in *Knotts* to a "dragnet type" search was a reference to "mass surveillance." Rejecting this contention outright, the Court stated: "Although the Government, focusing upon the term 'dragnet,' suggests *Knotts* reserved the Fourth Amendment question that would be raised by mass surveillance, not the question raised by prolonged surveillance of a single individual, that is not what happened. In reserving the 'dragnet' question, the Court was not only addressing but in part actually quoting the defendant's argument that, if a warrant is not required, then pro-longed 'twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision.' *Id.* at 283." *Id.* at 615 F.3d at 303-304.

totality of Jones's movements over the course of a month - was not exposed to the public: First, unlike one's movements during a single journey, the whole of one's movements over the course of a month is not actually exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed constructively even though each individual movement is exposed, because that whole reveals more - sometimes a great deal more - than does the sum of its parts." *Id.* at 558. The Court went on to explain – in response to the Government's argument that Jones' movements could have theoretically been physically observed by another person(s) – that the issue was one of reasonable expectation not what might be actually physically possible. As Judge Ginsburg responded: "The Government implicitly poses the wrong question… [i]n considering whether something is 'exposed' to the public as that term was used in *Katz* we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do." *Id.* at 559. "A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.'" *Id*. at 563.

Endorsing the "mosaic theory" to analyze the Fourth Amendment issues presented, the Court in *Maynard* explained that "mosaic theory" embodies the proposition that: "What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene." *Id.* at 562. At the Court noted:

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's

> movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups -- and not just one such fact about a person, but all such facts. *Id.* at 562.

Thus the *Maynard* Court found, for the reasons set forth above, that Jones did have an expectation of privacy over his movements for the month long period that he was tracked.

The Court then turned to the second part of the *Katz* test – was that expectation of privacy objectively reasonable? The Court found that the second part of the *Katz* test had been satisfied as well, reasoning that; "[a]pplication of the test in *Katz* and its sequellae to the facts of this case can lead to only one conclusion: Society recognizes Jones's expectation of privacy in his movements over the course of a month as reasonable, and the use of the GPS device to monitor those movements defeated that reasonable expectation. As we have discussed, prolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have - short perhaps of his spouse. The intrusion such monitoring makes into the subject's private affairs stands in stark contrast to the relatively brief intrusion at issue in *Knotts*; indeed it exceeds the intrusions occasioned by every police practice the Supreme Court has deemed a search under *Katz*." *Id.* at 563.

The Supreme Court granted certiorari in *Jones*. Justice Scalia, delivered the opinion of the Court, in which Justices Roberts, C.J., Kennedy, Thomas, and Sotomayor, joined. Justice Sotomayor, filed a concurring opinion and Mr. Justice Alito filed an opinion concurring in the judgment, in which Justices Ginsburg, Breyer and Kagan, joined.

Justice Scalia purposefully avoided analyzing the facts under the *Katz* test. Rather, he based his opinion exclusively upon a trespassory analysis, holding that the placement of the GPS tracking

devise in Jones' car violated the Fourth Amendment because "[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area… a search has undoubtedly occurred." *Id.* 132 S. Ct. at 951. He distinguished *Knotts* or *Kayo* as non-dispositive on the grounds that in each instance the beepers had been placed in containers that belonged to third parties – so the question of whether there was a trespassory violation of the Fourth Amendment never arose. *Id.* at 951-952.

Justice Alito, with whom Justice Ginsburg, Justice Breyer, and Justice Kagan joined, wrote a strong concurring opinion. Justice Alito made clear from the outset that it was his view that the case should be resolved on the basis of a *Katz* analysis, rather than by application of (antiquated) trespassory doctrine. "This case requires us to apply the Fourth Amendment's prohibition of unreasonable searches and seizures to a 21st-century surveillance technique, the use of a Global Positioning System (GPS) device to monitor a vehicle's movements for an extended period of time. Ironically, the Court has chosen to decide this case based on 18th-century tort law." *Id*. at 958.

Justice Alito criticized Justice Scalia's opinion for predicating the holding of a case of such self-evident importance on the happening of an event - placing a GPS device on an automobile while it was in a public place - "generally regarded as so trivial that it does not provide a basis for recovery under modern tort law." *Id.* at 961. In addition, he remarked that the Court was seemingly engaged in the same type of stagnation that had marked the early days of wiretapping cases - at first insisting that remediation had to be linked to some tangible act of trespass - and only many years later, finally adopting the *Katz* expectation of privacy test. *Id.* at 959.

In conclusion, Justice Alito and the four Justices who joined his concurring opinion held that: "[T]he use of longer term GPS monitoring in investigations of most offenses impinges on

expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not - and indeed, in the main, simply could not secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving… the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment." *Id.* at 964.

But perhaps the strongest views on these issues were expressed by Justice Sotomayor in her separate concurring opinion. Justice Sotomayor began by explaining that she felt compelled to write separately because "the Fourth Amendment is not concerned only with trespassory intrusions on property… even in the absence of a trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable…' [and that] [i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion property, the majority opinion's trespassory test may provide little guidance" *Id.* at 954-955.

Next, Justice Sotomayor – recognizing the place that technology and electronic devices have come to occupy in our society – candidly acknowledged that the (Third Party/Assumption of Risk) propositions that any information voluntarily disclosed to third parties should somehow be deemed to have lost any reasonable expectation of privacy – may no longer be viable in present day (precisely because of the ubiquity of electronic devices and the nature of how they operate and the citizenry's dependence on them). As Justice Sotomayor explained: "*More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties*. E.g., *Smith,* 442 U.S., at 742, 99 S. Ct. 2577, 61 L. Ed. 2d 220; *United States v. Miller*, 425 U.S. 435, 443, 96 S. Ct. 1619, 48 L. Ed.

2d 71 (1976). *This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers*." *Id.* at 957 (emphasis supplied).

Justice Sotomayor went on to explain that in attempting to resolve the calculus of whether; (1) someone had an expectation of privacy in his location and movements over a protracted period of time, and (2) whether in contemporary society that expectation would be regarded as objectively "reasonable" – it was her considered view that the conduct at bar met the *Katz* two part test and constituted a Fourth Amendment violation. As she explained: "I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year." *Id.* at 957.

In her opinion, Justice Sotomayor made two final points that are particularly relevant to consideration of the present case. First, she explained that the day had come to revisit the notion that complete "secrecy" was somehow a condition precedent to a finding of an expectation of privacy. As she noted, "whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *Id.* at 926. Second, she recognized that if the government is allowed to continue to ratchet-up its surveillance of the citizenry using the ever growing and ever more sophisticated array of electronic surveillance devices at its disposal – and those activities go on

essentially unmonitored and unchecked by meaningful judicial restraint and review - it could have a profoundly chilling effect on the fundamental liberties that are guaranteed by the First Amendment. As Justice Sotomayor wrote: "[B]y making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track - may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" *Id.* at 925.

Riley v. California

In a case that some observers have called "a ringing endorsement of privacy in the digital age,"[6] the Court in *Riley v. California*, ___ U.S. ___, 134 S. Ct. 2473 (2014) observed that: "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life' (*Id.* at 2495)… [a]ccording to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower (*Id.* at 2490)… [h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* at 2490.

In *Riley*, the Court held that the police must obtain a search warrant prior to examining the contents of a cell phone which they have seized incident to an arrest. What is interesting in *Riley*, as it relates to the issues in this case, is that in *Riley* the Court rejected the Government's argument that call logs and other metadata were not deserving of Fourth Amendment protection. Indeed, Justice Robert's opinion took aim at the third-party doctrine – that "non-content" records like call

[6] Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond The Content/Non-Content Distinction*, 54 Santa Clara L. Rev. 821, 838 (2014).

logs, location data, and other metadata held by third parties can be collected by the government without a warrant. Non-content "found on an Internet-enabled phone… could reveal an individual's private interests or concerns… [h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* at 2490.

Relevant State Court Decisions

In 2013 the Supreme Court of the State of New Jersey decided *State v. Earls*, 214 N.J. 564, 70 A.3d 630 (2013). In *Earls*, the Court held that obtaining cell site location information without first obtaining a judicial warrant was a violation of Article I, Paragraph 7 of the New Jersey Constitution. To wit:

> For the reasons discussed, we conclude that Article I, Paragraph 7 of the New Jersey Constitution protects an individual's privacy interest in the location of his or her cell phone. Users are reasonably entitled to expect confidentiality in the ever-increasing level of detail that cell phones can reveal about their lives. Because of the nature of the intrusion, and the corresponding, legitimate privacy interest at stake, we hold today that police must obtain a warrant based on a showing of probable cause, or qualify for an exception to the warrant requirement, to obtain tracking information through the use of a cell phone. *Id.* at 588.

One of the most notable components of the reasoning expressed in Chief Judge Rabner's opinion (writing for a unanimous Court), was the Court's outright rejection of the continuing viability of the Third Party Disclosure doctrine. As the Court held unequivocally: "*At the outset, we note that an individual's privacy interest under New Jersey law does not turn on whether he or she is required to disclose information to third-party providers to obtain service. When people make disclosures to phone companies and other providers to use their services, they are not promoting the release of personal information to others*." *Id*. at 584 (emphasis supplied).

Further, in assessing whether people have an subjective expectation of privacy in their historical cell phone data – and whether such an expectation was objectively "reasonable – the

Court noted: "[P]eople do not buy cell phones to serve as tracking devices or reasonably expect them to be used by the government in that way. We therefore find that individuals have a reasonable expectation of privacy in the location of their cell phones under the State Constitution." *Id.* at 568-569. Indeed, the Court went on to explain that: "Just as customers must disclose details about their personal finances to the bank that manages their checking accounts, cell-phone users have no choice but to reveal certain information to their cellular provider. That is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not using a cell phone… [w]hen people make disclosures to phone companies and other providers to use their services, they are not promoting the release of personal information to others." *Id.* at 584.

In expressing its findings as to the magnitude of the invasion of privacy takes place when a person's historical cell phone information is gathered and analyzed. The Court "note[ed] that disclosure of cell-phone location information, which cell-phone users must provide to receive service, can reveal a great deal of personal information about an individual. With increasing accuracy, cell phones can now trace our daily movements and disclose not only where individuals are located at a point in time but also which shops, doctors, religious services, and political events they go to, and with whom they choose to associate. That information cuts across a broad range of personal ties with family, friends, political groups, health care providers, and others." *Id*. at 586.

In *Commonwealth v. Augustine*, 467 Mass. 230, 4 N.E.3d 846 (2014) an Assistant District Attorney in Middlesex County Massachusetts – in furtherance of a murder investigation - sought and obtained a D-Order to acquire a putative defendant's historical CSLI for a 14 day time period. *Id.* at 233. After his arrest, the Defendant moved to suppress the CSLI on the grounds that it was obtained in violation of his rights under the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights. After a hearing, the Court allowed the

defendant's motion, concluding that "at least under art. 14 of the Massachusetts Declaration [of] Rights there was a search such that this information must be suppressed." *Id.* at 234. The Commonwealth filed an application for interlocutory review and a single justice allowed the case to be heard by the Massachusetts Supreme Court. *Id.* at 234.

The Massachusetts Supreme Court began by acknowledging that 18 U.S.C. §2703(d) applied to instances in which a governmental agency sought permission to obtain CSLI. *Id.* at 235-237. Moreover, both the prosecution and the defense agreed that "the § 2703(d) order issued by the Superior Court judge was valid insofar as it was based on a showing of 'specific and articulable facts showing that there are reasonable grounds to believe' that the CSLI records sought were relevant and material to an ongoing criminal investigation.'" *Id.* at 236. The issue framed for the Court however was weather under federal or Massachusetts constitutional law, historical CSLI could be obtained without first securing a warrant based upon a showing of probable cause. *Id*. at 236.

Initiating its analysis of the issues, the Court found that technology had reached the point by 2014, that law enforcement agencies had the ability to precisely determine and historically track a person's location with chilling precision. "[A]s the motion judge observed, when the government obtains historical CSLI from a cellular service provider, the government is able to track and reconstruct a person's past movements, a category of information that never would be available through the use of traditional law enforcement tools of investigation. Furthermore, as discussed previously, cellular telephone location tracking and the creation of CSLI can indeed be more intrusive than GPS vehicle tracking." *Id*. at 254.

In opposition, the Commonwealth raised three arguments. First, it claimed that "state action" was not involved, since it was the defendant's cell phone provider (Sprint) and not the

Commonwealth of Massachusetts that had captured and collected the defendant's CSLI. *Id*. at 240. The Court dispatched that argument rather quickly, finding that, "through a court order, the Commonwealth compelled Sprint to turn over the defendant's CSLI. Because the § 2703(d) order required the CSLI disclosure and [since] a search was 'instigated' by the Commonwealth, State action clearly was involved." *Id*. at 241.

The second argument advanced against suppression was based upon the Third Party Disclosure doctrine. *Id.* at 242-24 Although conceding that in the past the Court had followed the reasoning in *Smith* and *Miller* in applying its Fourth Amendment jurisprudence (*Id.* at 244), the Court expressly found that the Third Party Disclosure doctrine – in light of the self-evident technological advances which had taken place – simply could no longer be applied to justify a finding that a cell phone user had (knowingly and voluntarily) assumed the risk that his cell phone provider would reveal his CSLI to the police. As the Court held: "*We agree with the defendant, however, that the nature of cellular telephone technology and CSLI and the character of cellular telephone use in our current society render the third-party doctrine of Miller and Smith inapposite; the digital age has altered dramatically the societal landscape from the 1970s*." *Id.* at 245 (emphasis supplied). The Court went on to enumerate a number of reasons why the doctrines formulated in *Miller* and *Smith* were inapplicable to the issue of historical CSLI. As the Court explained.

> We find a significant difference between the two. In *Smith*, the information and related record sought by the government, namely, the record of telephone numbers dialed, was exactly the same information that the telephone subscriber had knowingly provided to the telephone company when he took the affirmative step of dialing the calls. The information conveyed also was central to the subscriber's primary purpose for owning and using the cellular telephone: to communicate with others. No cellular telephone user, however, voluntarily conveys CSLI to his or her cellular service provider in the sense that he or she first identifies a discrete item of information or data point like a telephone number… and then transmits it to the provider. CSLI is purely a function and product of cellular telephone technology,

> created by the provider's system network at the time that a cellular telephone call connects to a cell site. And at least with respect to calls received but not answered, this information would be unknown and unknowable to the telephone user in advance -- or probably at any time until he or she receives a copy of the CSLI record itself. Moreover, it is of course the case that CSLI has no connection at all to the reason people use cellular telephones. See *Earls*, 214 N.J. at 587 ("People buy [cellular telephones] to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a [cellular telephone] to share detailed information about their whereabouts with the police"). Moreover, the government here is not seeking to obtain information provided to the cellular service provider by the defendant. Rather, it is looking only for the location-identifying by-product of the cellular telephone technology - a serendipitous (but welcome) gift to law enforcement investigations. Finally, in terms of the privacy interest at stake here - the individual's justifiable interest in not having "his comings and goings… continuously and contemporaneously monitored" by the government… the enormous difference between the cellular telephone in this case and the "land line" telephone in *Smith* seems very relevant. In terms of location, a call log relating to a land line may indicate whether the subscriber is at home, but no more. But for a cellular telephone user carrying a telephone handset (as the defendant was), even CSLI limited to the cell site locations of telephone calls made and received may yield a treasure trove of very detailed and extensive information about the individual's "comings and goings" in both public and private places; in this case, as mentioned, the defendant's CSLI obtained by the Commonwealth covered at least sixty-four pages. *Id.* at 249-251.

Addressing the constitutional significance of the length of time that the records would allow the police to historically track the defendant, the Court opined that: "[T]here is no need to consider at this juncture what the boundaries of such a time period might be in this case because, for all the reasons previously rehearsed concerning the extent and character of cellular telephone use, the two weeks covered by the § 2703(d) order at issue exceeds it: even though restricted to telephone calls sent and received (answered or unanswered), the tracking of the defendant's movements in the urban Boston area for two weeks was more than sufficient to intrude upon the defendant's expectation of privacy safeguarded by art. 14." *Id.* at 255-256.

In conclusion, the Court held that: "the defendant made a showing of a subjective privacy interest in his location information reflected in the CSLI records, and for all the reasons we have considered here, we conclude that this interest is one that our society is prepared to recognize as

reasonable… [a]ccordingly, the government-compelled production of the defendant's CSLI records by Sprint constituted a search in the constitutional sense to which the warrant requirement of art. 14 applied." *Id.* at 255. Accord: *Commonwealth v. Wyatt*, 30 Mass. L. Rep. 270, 2012 Mass. Super. LEXIS 248 (Mass. Super. Ct. 2012).

Tracy v. Florida, 152 So. 3d 504, 2014 Fla. LEXIS 3072 (2014), was a case which focused on real-time cell phone location tracking rather than the acquisition of historical CSLI, but is nonetheless an important decision for this Court to consider, because it too, found that application of the Third Party Disclosure doctrine is simply no longer viable given the dependence upon cell phone technology in present times.

The Court in *Tracy* echoed the sentiments of Justice Sotomayor in *Jones*, that the *Katz* expectation of privacy calculation cannot depend on secrecy as a, *per se*, indispensable requirement. As Chief Judge Labarga, writing the opinion for the majority in *Tracy* reasoned: "[As Justice Sotomayor] aptly noted, [w]hatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *Id*. at 520. The Court went on to expressly endorse the reoccurring conclusion reached in so many recent cases - that people simply cannot be expected to choose between withdrawing from commerce and society as the only solution to protect their privacy. For better or for worse, cell phones have become, a necessary extension of the person. It is how people communicate, research, navigate, engage in commerce, etc. As the Court found:

> It is true that a cell phone user can prevent locational signals from being used for tracking purposes by turning off the cell phone, thus concealing the signals and the location of the user. However, we do not find that such concealment is a necessary predicate to the Fourth Amendment claim presented under the facts of this case.

> We have previously recognized that in addition to using cell phones to make telephone calls, "a significant portion of our population relies upon cell phones for email communications, text-messaging information, scheduling, and banking." Smallwood, 113 So. 3d at 733. Requiring a cell phone user to turn off the cell phone just to assure privacy from governmental intrusion that can reveal a detailed and intimate picture of the user's life places an unreasonable burden on the user to forego necessary use of his cell phone, a device now considered essential by much of the populace. "The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone must be rejected." *Id.* at 523.

Judge Labarga, writing for the Court, concluded with the observation that: "we conclude that such a subjective expectation of privacy of location as signaled by one's cell phone - even on public roads - is an expectation of privacy that society is now prepared to recognize as objectively reasonable under the *Katz* 'reasonable expectation of privacy' test." *Id.* at 526.

The Decisions by the New York State Court of Appeals in *People v. Weaver* and *Matter of Cunningham v New York State Dept. of Labor*

The opinion by the New York State Court of Appeals in *People v. Weaver*, 12 N.Y.3d 433, 882 N.Y.S.2d 357 (2009) begins with the factual recital that in "the early morning hours of December 21, 2005, a State Police Investigator crept underneath defendant's street-parked van and placed a global positioning system (GPS) tracking device inside the bumper. The device remained in place for 65 days, constantly monitoring the position of the van. This nonstop surveillance was conducted without a warrant." *Id.*at 436.

At the trial, without even conducting a hearing, the trial court denied the Defendant's motion to suppress the GPS data. *Id.* at 436. Following his conviction, the Defendant prosecuted an appeal to the Appellate Division, Third Department. *Id.* at 438. In a four to one decision, the Third Department affirmed the trial court. (*People v. Weaver*, 52 A.D.3d 138, 860 N.Y.S.2d 223 [3d Dep't. 2008]). The Appellate Division based their decision on the assertion that: "[A] defendant has no reasonable expectation of privacy in the publicly accessible exterior of his or her

vehicle, and the undercarriage is part of the vehicle's exterior… [n]or can defendant expect privacy as to the location of his or her vehicle on public streets." *Id*. 52 A.D.3d at 141. The Court went on to hold that under the New York Constitution (Art 1, § 12), "our state constitutional law should 'focus on whether there has been an intrusion into an area where an individual has a reasonable expectation of privacy.'" *Id*. at 143.

Appellate Division Justice Leslie Stein was the single dissenter. She wrote that while she would agree that federal Fourth Amendment jurisprudence would compel the decision reached by the majority, New York State Fourth Amendment jurisprudence required a different finding. *Id*. at 143-144. Justice Stein explained that under New York law, "*while the citizens of this state may not have a reasonable expectation of privacy in a public place at any particular moment, they do have a reasonable expectation that their every move will not be continuously and indefinitely monitored by a technical device without their knowledge, except where a warrant has been issued based on probable cause… At some point, the enhancement of our ability to observe by the use of technological advances compels us to view differently the circumstances in which an expectation of privacy is reasonable. In my opinion, that point has been reached in the facts before us. Thus, where, as here, no warrant was issued authorizing the placement of the GPS device on defendant's car, I would find that defendant's rights against unreasonable search and seizure under NY Constitution, article I, § 12 were violated" Id*. at 145-146 (emphasis supplied).[7] Justice Stein, granted leave to the Court of Appeals to hear the appeal. (See, CPL § 460.20 [2][a]).

[7] Justice Stein has now been elevated to the New York State of Appeals. At the time that the Court decided *People v. Weaver*, 12 N.Y.3d 433 (2009), the majority opinion was delivered by Chief Judge Lippman, in which Judges Ciparick, Pigott and Jones concurred. Judge Smith dissented in an opinion in which Judges Graffeo and Read concurred. Judge Read dissented in an opinion in which Judge Graffeo concurred. The makeup of the Court since *Weaver* however has changed. Judges Smith, Graffeo (dissenters in *Weaver*) are gone. Judge Read is the only dissenter who remains on the bench today. Judge Leslie E. Stein (whose dissenting opinion in *Weaver* in Third

Rejecting the reasoning of the Appellate Division, the Court of Appeals agreed with Justice Stein's analysis as to the nature of the expectations of privacy that a New York citizen could reasonably and justifiably harbor. Discussing the technological advances that had taken place since the Supreme Court's decision in *Knotts*. The Court noted: "Constant, relentless tracking of anything is now not merely possible but entirely practicable, indeed much more practicable than the surveillance conducted in *Knotts*. GPS is not a mere enhancement of human sensory capacity, it facilitates a new technological perception of the world in which the situation of any object may be followed and exhaustively recorded over, in most cases, a practically unlimited period." *Id.* 12 N.Y.3d 441.

As Chief Judge Lippman, pointed out, the State of New York was far quicker to embrace the interpretation and application of the Fourth Amendment championed by Mr. Justice Brandeis in his dissent in *Olmstead*, than were the federal courts. As Judge Lippman recounted: "Brandeis's dissent was resonant … some 12 years later, at the New York State Constitutional Convention of 1938, the view that there should be constitutional protection against governmental infringements of privacy not involving any offense against property found vindication in this state's analogue to the Fourth Amendment, only then adopted. Our constitutional provision (art I, § 12), in addition to tracking the language of the Fourth Amendment, provides: 'The right of the people to be secure against unreasonable interception of telephone and telegraph communications shall not be violated, and ex parte orders or warrants shall issue only upon oath or affirmation that there is reasonable ground to believe that evidence of crime may be thus obtained, and identifying the

---

Department was ultimately adopted by the Court of Appeals), as well as Judges Sheila Abdus-Salaam (who wrote a separate concurring opinion in *Matter of Cunningham v. New York State Dept. of Labor)* and Eugene M. Fahey have now joined the bench.

particular means of communication, and particularly describing the person or per-sons whose communications are to be intercepted and the purpose thereof.'" *Id.* at 438-439.

In conclusion, the Court found that the 65 day period for which surveillance data was gathered amounted to a "dragnet use of the technology," that was "*not consistent with the values at the core of our State Constitution's prohibition against unreasonable searches*." *Id*. at 446 (emphasis supplied). The Court directed that order of the Appellate Division be reversed, that the Defendant's motion to suppress should be granted and a new trial was ordered. *Id*. at 447.

In 2013, the Court of Appeals decided *Matter of Cunningham v. New York State Dept. of Labor*, 21 N.Y.3d 515, 974 N.Y.S.2d 896 (2013). That case involved the installation of a GPS tracking device on the automobile of the Director of Staff and Organizational Development of the State Department of Labor, a New York State employee. The device monitored the movements of the employee's car for a month. *Id*. at 518. The GPS tracking data documented the employee's times of arrival and departure from his office, and was also used to compare the Director's approval of time records showing his secretary was working during hours when the GPS information showed that he was visiting her home. On the basis of this information – and following a hearing – the Director was terminated and he subsequently brought an Article 78 proceeding challenging the ruling of the Commissioner of Labor. *Id*. at 519.

While both sides conceded that under the *Weaver* and the subsequent decision by the Supreme Court in *Jones*, the warrantless monitoring of the employee's car – without obtaining a warrant – was a violation of both state and federal constitutional law (*Id*. at 520) the issue which had to be resolved, was whether the "workplace exception to the warrant requirement" required a different result. *Id*. at 520. Examining the elements of the "workplace" exception the Court pointed out that one of the requirements for application of the exception was that the search was

"reasonable in its scope." *Id*. at. 522. While the Court acknowledged that none of the evidence gathered by the GPS search concerned instances that were outside of business hours, "GPS searches like the present one, in light of the extraordinary capacity of a GPS device to permit '[c]onstant, relentless tracking of anything,'" rendered the search "unreasonable," and therefore unconstitutional, under New York State law. *Id*. at 523.

In a strong concurring opinion by Judge Abdus-Salaam, she emphasized the invasiveness that this type of prolonged surveillance (for a 30 day period) had upon settled concepts of privacy. Relying on the Court's prior holding in *Weaver* and Justice Sotomayor's concurring opinion in *Jones*, Judge Abdus-Salaam wrote: "It took 'little imagination' for us to conjure the types of 'indisputably private' information that would be '[d]isclosed in the data' from a GPS device planted on a person's vehicle: '[T]rips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on. What the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations--political, religious, amicable and amorous, to name only a few - and of the pattern of our professional and avocational pursuits" (id. at 441-442; see *Jones*, 565 US ___, 132 S Ct at 955 [Sotomayor, J., concurring] [citing *Weaver* for the proposition that 'GPS monitoring generates a precise, comprehensive record of a person's public.'" *Id*. at 524-525.

Other New York Decisions Which Relate to the Issues Before the Court

In *People v. Hall*, 86 A.D. 3d 450, 926 N.Y.S. 2d 514 (1st Dep't. 2011) the Appellate Division considered a case in which the facts showed that in the early morning hours of October 12, 2005, the defendant opened fire on a group of patrons who had just left a night club. One bullet

struck the mother of a seven-year-old boy, piercing her lung and causing her death. Another round struck a homeless man in the leg, shattering his bone. A third victim was injured by a bullet that passed through his calf and another that grazed his finger. *Id. at 450*. The police made an application under the Stored Communications Act, Section 2703(d) to obtain Cell Site Location Information for the three day period surrounding the October 12th shooting date. *Id. at 451*.

The Court held that it was unnecessary to obtain a warrant to acquire the defendant's CSLI because he had "no reasonable expectation of privacy while traveling in public" - citing the decisions in *United States v Knotts*, 460 US 276, 281, 103 S Ct 1081 (1983) and *In re Application of US for Order Directing Provider of Elec. Communication Serv. to Disclose Records to Govt.*, 620 F3d 304, 308-310 (3d Cir. 2010). Although the Court wrote that it was rejecting appellant's argument that suppression was required under the New York State Constitution (and consistent with *People v. Weaver, supra*.) because it was "unpreserved," and further that the Court "declin[ed] to review it in the interests of justice" (*Id. at 452)*, having once said that, the Court nevertheless went on reach the claim on the merits:

> As an alternative holding, we reject it on the merits. Although *Weaver* requires the police to obtain a warrant supported by probable cause for the installation of a global positioning system device, it does not address the matter of CSLI records. Additionally, in *Weaver the device was used to track the defendant's movements for 65 days, as opposed to a mere 3 days in the instant case. To the extent that prolonged surveillance might require a warrant under federal law* (see *United States v Maynard*, 615 F3d 544, 392 US App DC 291 [DC Cir 2010], cert denied 562 US ___, 131 S Ct 671, 178 L Ed 2d 500 [2010]), *we find that three days of CSLI records does not constitute a protracted surveillance*. *Id at 452*. (emphasis supplied)

Of course the period of surveillance in the instant case was vastly longer than that in *Hall* – 3 days in *Hall* as compared to 201 days in this case. And as the Appellate Division observed, "prolonged surveillance might require a warrant under federal law (citations omitted) we find that three days of CSLI records does not constitute a protracted surveillance" *Id*. at 452.

Although when the Appellate Division decided *Hall* it did not have the benefit of the Supreme Court's decision in *Jones*, there is actually little tension between the two decisions. That is to say, in *Hall* the Appellate Division focused on the very short duration for which the CSLI was obtained (3 days), finding that such conduct did not offend either state or federal constitutional boundaries. At the same time, the Court expressly recognized and acknowledged that if the surveillance had lasted for a substantially longer period, a different constitutional result would have obtained. This reasoning is entirely consistent with Justice Alito's concurrence in *Jones* when he observed that: "Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. See *Knotts*, 460 U.S., at 281-282, 103 S. Ct. 1081, 75 L. Ed. 2d 55. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not - and indeed, in the main, simply could not secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark." *Jones*, 132 S. Ct. at 964.

Nor did the Appellate Division in *Hall* have the benefit of the subsequent Court of Appeals decision in *Matter of Cunningham v. New York State Dept. of Labor*, *supra*, in which the Court found that conducting "seven-day, 24-hour surveillance for a full month," constituted an unreasonable search in the absence of a judicial warrant. *Id*. 21 N.Y.3d at 523.

People v. Watkins, 125 A.D.3d 1364, 2015 N.Y. App. Div. LEXIS 1102 (4th Dep't. 2015) was a case decided by the Appellate Division Fourth Department which concerned the real-time

(or as it is sometimes referred to, "prospective") acquisition of CSLI. However the Court resolved the case by application of the "exigent circumstances" exception to the warrant requirement. As the Court held: "Even assuming, arguendo, that the use of that technique constituted a search implicating the protections of the Federal and State Constitutions (see US Const, 4th Amend; NY Const, art I, § 12), we conclude that the People established that exigent circumstances justified the police in proceeding without a warrant."

In *People v. Moorer*, 39 Misc. 3d 603, 959 N.Y.S.2d 868 (County Ct., Monroe Ct. 2013) the police were conducting a homicide investigation in an effort to locate the individual suspected of having committed a murder. The police obtained historical CSLI from Sprint on the basis of an "Exigent Circumstances Request." *Id*. at 605. By proactively "pinging" the Defendant's cell phone on two separate occasions, they were eventually able to locate it in a knapsack found in a room the defendant sometimes occupied at his grandmother's home. *Id*. at 606. The defendant was subsequently arrested and moved to suppress the CSLI evidence that had been obtained.

The People argued first that "pinging" was permissible under the Stored Communications Act because "exigent circumstances" existed. The Court rejected the People's argument on the grounds that to qualify for an "exigent circumstances" exception there had to be a showing that an "immediate danger of death or serious bodily injury" and "[t]he pinging here was sought to permit the investigators to locate defendant's cell phone; under these facts, clearly not an exigent circumstance." *Id*. at 610. The Court went on to hold however, that "searches that are conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule (see *Davis v United States*, ___U.S. ___ , 131 S Ct 2419, 180 L. Ed. 2d 285 [2011])." *Id*. at 616.

Most respectfully the Court's reliance on a "good faith" exception to the exclusionary rule is of questionable validity given the fact that the New York State Court of Appeals has expressly rejected the "good faith exception" on the basis of the New York State Constitution. See, *People Bigelow*, 66 N.Y.2d 417, 497 N.Y.S.2d 630 (1985): "We therefore decline, on State constitutional grounds, to apply the good faith exception the Supreme Court stated in *United States v Leo*n (*supra*)." *Id*. at 427.

The Court in *Moorer* went on to make the finding that "public ignorance about cell phone technology can no longer be maintained in this day and age - cell phones are voluntarily carried by their users and may be turned on or off at will… [b]y a person's voluntary utilization, through GPS technology, of a cell phone, a person necessarily has no reasonable expectation of privacy with respect to the phone's location." *Id*. at 618. The validity of this conclusion too, however, is called into question. The Court does not explain the basis for its finding, and does not provide any authority for its *ipse dixit* contention. Cf., *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Services to Disclose Records to the Government*, 620 F.3d 304, 317-318 (3rd Cir. 2010): "A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way… [I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, '[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all.'" *Id*. at 317-318; *Commonwealth v. Pitt*, 29 Mass. L. Rep. 445, 2012 Mass. Super. LEXIS 39 (Mass. Super. Ct. 2012): "Unlike the affirmative gesture of conveying dialed phone numbers to a third-party

telephone service provider, a cell phone subscriber takes no overt steps to communicate his physical location to a cell phone service provider. In fact, '[i]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information." *Id*.at 11.

In *People v Wells*, 45 Misc. 3d 793, 991 N.Y.S.2d 743 (Sup. Ct. Queens Cty. 2014), the Court denied a motion to suppress on the basis of its finding that: "And of great concern to the courts presently, there was no 'tracking' of the defendant's calls or his location over an extensive period of time without a warrant … [t]he mere 'pinging' of his cell phone to obtain one-time location information is not a search." *Id*. at 797.

Technological Advances Continue to Require the Evolution and Recalibration of Fourth Amendment Doctrine

As a historical review of Fourth Amendment jurisprudence reveals – at least as far as federal constitutional law is concerned – for nearly 200 years, it was primarily grounded in trespassory analysis. Some type of physical intrusion into a protected place (or someone's effects) had to occur to trigger exclusionary rule remediation. Yet the storm warnings that technology would outstrip the mechanisms in place to guard the privacy of the citizenry were heard as early as Justice Brandeis's dissenting opinion in *Olmstead.* As Justice Brandeis forewarned: "[T]ime works changes, brings into existence new conditions and purposes. Subtler and more far-reaching means of invading privacy have become available to the Government… 'in the application of a constitution, our contemplation cannot be only of what has been but of what may be.' The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping." *Olmstead*, 277 U.S. at 473-474 (Brandeis, J. dissenting).

Nevertheless, it would not be until the 1967 decision in *Katz* that the Court would finally shed the yoke of trespassory doctrine and embrace the view of Justice Brandeis that Fourth

Amendment privacy violations can occur without physical intrusions. Thus Katz brought about the first major transformation of Fourth Amendment jurisprudence from a dogmatically trespassory construction and application, to the recognition that the Constitution protects people's privacy, not just people's private places. To wit: "We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling." *Id. Katz*, 389 U.S. 353.

It is imperative that the Fourth Amendment keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.[8] See *Kyllo v. United States*, 533 U.S. 27, 34, 121 S. Ct. 2038 (2001) (noting that evolving technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment") *Id*. at 285

In *Jones*, both Justice Alito and Justice Sotomayor stressed the pressure that advancing technology was putting upon Fourth Amendment *stare decisis*.[9]

The New York Court of Appeals too - in its decisions in both *Weaver* and *Matter of Cunningham v. New York State Dept. of Labor* – clearly voiced its concern over the threat that the

[8] As the Court in *In re Cellular Tels.*, 2014 U.S. Dist. LEXIS 182165, 11-12 (D. Kan. 2014) recently warned: "With technological developments moving at such a rapid pace, Supreme Court precedent is and will inevitably continue to be absent with regard to many issues district courts encounter. As a result, an observable gap has arisen between the well-established rules lower courts have and the ones they need in the realm of technology. Courts cannot, however, allow the existence of that gap to infiltrate their decisions in a way that compromises the integrity and objectives of the Fourth Amendment. As the Supreme Court stated in *Riley*, '[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.' The danger, of course, is that courts will rely on inapt analogical reasoning and outdated precedent to reach their decisions. To avoid this potential pitfall, courts must be aware of the danger and strive to avoid it by resisting the temptation to rationalize the application of ill-fitting precedent to circumstances."

[9] Miriam H. Baer, *Secrecy, Intimacy, and Workable Rules: Justice Sotomayor Stakes Out the Middle Ground in United States v. Jones*, 123 Yale L.J. F. 393 (2014).

ever increasing sophistication (coupled with ease of use and the relative inexpensive operation) that law enforcement surveillance devices pose to the privacy of the people in this State.

And now courts must confront yet another manifestation of law enforcement's seeming insatiable preoccupation with the surveillance of its citizens (and with the collection of every manner and sort of data about their activities) - and that is the threat now presented by wholesale data collection, location tracking, and data mining.

In that regard, the collection of "location tracking" data can take several forms. First, there is so-called "real-time" location tracking. This can be carried out in any number of ways; i.e. by using either a concealed GPS tracking device; by using the GPS capabilities of an individual's smartphone; by "pinging" a cell phone to determine what tower it registers to; or through the use of IMSI catchers (International Mobile Subscriber Identity) – sometimes referred to as a "StingRay devices" or "dirtboxs."[10] Second, "location tracking" can be very effectively accomplished – and is perhaps most commonly accomplished - through the acquisition of historical CSLI data. And depending on the length of time for which such information is gathered, very detailed location tracking is possible. (See brief of *amici* at pp. 19-21).

This Court Should Apply Mosaic Theory to Resolve Whether The Acquisition of Defendant's Historical CSLI Data was a "Search" Within the Meaning of the 4th Amendment and/or Art. 1, § 12 of the N.Y. Constitution

In assessing the magnitude of any potential invasion of privacy that may be occasioned by prolonged location tracking, a number of courts have turned to so-called "Mosaic Theory" analysis.

[10] See, Steven M. Bellovin, *When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J.L. & Liberty 556 (2014).

The term "mosaic theory" was first used in connection with Fourth Amendment analysis by Judge Ginsburg of the District of Columbia Court of Appeals in *United States v. Maynard*.[11] As the Court explained:

> As with the "mosaic theory" often invoked by the Government in cases involving national security information, "What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene." (citations omitted) Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby sup-ply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups -- and not just one such fact about a person, but all such facts. *Id*. 615 F. 3d at 562.

The nature of the calculus performed under mosaic theory, is that the court looks not to the individual cell site location points in isolation, but rather to the comprehensive aggregation of that data. Given sufficient data location points – which, axiomatically, are a direct result of the length of time historical CSLI is obtained for - discrete units of surveillance data can be processed (either manually or through the application of various types of software) to create a highly detailed "mosaic," revealing virtually every aspect of an individual's movements, activities and associations.

Applying mosaic theory analytics, "a sequence of acts may constitute a Fourth Amendment search even if none of the individual acts trigger constitutional scrutiny."[12] The utilization of

---

[11] *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), aff'd sub nom. *Jones v. United States*, 565 U.S.___, 132 S. Ct. 945 (2012).

[12] *Id*. 8 NYU J.L. & Liberty 556, 571 (2014).

mosaic theory allows a court to identify the true measure of the invasion of privacy that has occurred because the composite image is revealed.[13] And thus the focus of the constitutional inquiry is whether the mosaic created by the aggregation of the multitude of independent location data points reveals so much private and intimate information about the individual, that; (1) his subjective expectation of privacy has been violated, and (2) that having identified the nature and magnitude of the invasion of privacy that has occurred, can it fairly be said that society would objectively find that the individual had – and was entitled – to a reasonable expectation of privacy with respect to the activities that have been revealed to law enforcement.

In *People v. Weaver* and *Matter of Cunningham v. New York State Dept. of Labor*, the Court of Appeals Applied Mosaic Theory to Resolve the "Reasonable Expectation of Privacy" Test of *Katz*

While the term "mosaic theory" may first have been used by Judge Ginsburg in *Maynard*, the fundamental analytics of mosaic theory were the basis for the holding by the New York Court of Appeals in its decisions in both *People v. Weaver* and *Matter of Cunningham v. New York State Dept. of Labor.*[14] That is to say, rather than viewing the location data which had been acquired from a *Knotts* perspective and finding that simply because the GPS device could locate a vehicle at some particular point in time on some public thoroughfare – which in itself might not be a particularly significant Fourth Amendment event since a human could make a similar observation

---

[13] *Ibid.* at 590.

[14] See also, *United States v. Katzin*, 732 F.3d 187, 238 n.23 (3d Cir. 2013): "[F]ive justices wrote or joined the concurring opinions in *Jones*, all of which seemed to endorse the so-called "mosaic" theory expressed in *Maynard* - which would unequivocally limit the holding in *Knotts* to apply in only short-term surveillance. See Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 326 (2012). This question does not need to be answered today; but emphasizes the major shift caused by *Jones* in Fourth Amendment law, and the vastly different legal regime under which the law enforcement officers here were acting." Also see, Ken Strutin, *Mosaic Theory: A New Perspective for Human Privacy*, (NYLJ 9/24/13)

– the Court embraced the notion that it was not any particular event in isolation that was significant, but the fact that all of the independent location points could be easily and inexpensively aggregated to produce a composite that was clearly greater than a sum of its parts. As the Court observed: "One need only consider what the police may learn, practically effortlessly, from planting a single device. The whole of a person's progress through the world, into both public and private spatial spheres, can be charted and recorded over lengthy periods possibly limited only by the need to change the transmitting unit's batteries… [w]hat the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations--political, religious, amicable and amorous, to name only a few--and of the pattern of our professional and avocational pursuits." *Weaver,* 12 N.Y. 3d at 443. Accord, *Matter of Cunningham v. New York State Dept. of Labor*, 21 N.Y. 3d 524-525. Also see, *Tracy v. Florida, supra*: "The theory that discrete acts of surveillance by law enforcement may be lawful in isolation, but may otherwise infringe on reasonable expectations of privacy in the aggregate because they 'paint an "intimate picture" of a defendant's life,' has been referred to as the 'mosaic" theory.'" *Id.* at 520.

This Court Should Apply Mosaic Theory to Determine the Instant Motion to Suppress

One of the criticisms of mosaic theory that has been raised by various Courts and in scholarly articles, is the conundrum of how are the temporal or composite boundaries to be determined. That is to say – when has law enforcement acquired ("seized") a sufficient amount of historical CSLI that the constitutional threshold has been passed. When there is sufficient information so that a decipherable montage is formed. As the Court noted in *United States v. White*, 2014 U.S. Dist. LEXIS 166444 (E.D. Mich. 2014): "There is a problem, of course, in deciding when the aggregation of data showing movement in public spaces crosses the line and becomes a

'search.' See, e.g., Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 330-36 (2012). However, courts have confronted similar problems in the past… [t]o find an answer, courts must 'balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.'" *Id.* at 18-19.

However in this regard, it is fair to observe that many of the quantitative standards that serve as the bedrock of our criminal justice system are applied *ad hoc* - based upon subjective judicial determinations - and yet they have well served for centuries, even though they lack the mathematical certainty that some critics of mosaic theory complain about. Consider for example, the lack of quantitate or qualitative parameters for such important legal standards as "proof beyond a reasonable doubt;" the standard necessary to make a showing of "probable cause;" when information said to support a search will be deemed sufficiently dated to be constitutionally "stale" – the examples of unquantifiable and subjectively applied standards abound.

In any event, while academics may debate when the point of critical mass is reached in mosaic theory (or the complexities of how that determination is made), under the facts presented by this case – what otherwise might be a thorny constitutional problem – is easily resolved.

In terms of what sort of a factual showing is probably insufficient, the Court may look to a number of New York state decisions: i.e., *People v. Hall, supra* at 452: "To the extent that prolonged surveillance might require a warrant under federal law… we find that three days of CSLI records does not constitute a protracted surveillance." Similarly, *People v. Watkins*, 125 A.D.3d 1364, 2015 N.Y. App. Div. LEXIS 1102 (4th Dep't. 2015): "Even assuming, arguendo, that the use of that technique constituted a search implicating the protections of the Federal and State Constitutions… we conclude that the People established that exigent circumstances justified

the police in proceeding without a warrant;" *People v. Moorer, supra*, where the Court distinguished obtaining several days of cell site location information from cases involving protracted location data acquisitions; To wit: "Defendant relies on opinions of several federal magistrates who denied the government's requests for a court order or a search warrant allowing the government to obtain prospective or real time cell site data for an extended period of time." *Moorer*, 39 Misc. 3d at 610. Also see, *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012): "While *Jones* involved intensive monitoring over a 28-day period, here the DEA agents only tracked Skinner's cell phone for three days. Such 'relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable.'" *Id*. at 780.

Correspondingly, on the – undoubtedly sufficient – side of the aisle, there is also meaningful guidance. In *Jones*, for example – and in direct response to the question posed by Justice Scalia of how long was long enough to trigger a Fourth Amendment violation, Justice Alito responded – unequivocally – *"relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable… [w]e need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.*" *Jones*, 132 S. Ct. at 964 (emphasis supplied). Justice Sotomayor expressed the same conclusion: "|I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy… In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention." *Id*. at 955.

The United States District Court for the District of Northern California recently held that the acquisition of 120 days of historical cell site data - by the use of a D-Order rather than a

judicially issued warrant – violated the Fourth Amendment. *United States v. Cooper*, 2015 U.S. Dist. LEXIS 25935, 15-27 (N.D. Cal. 2015). Also see, *United States v. Powell*, 943 F. Supp. 2d 759, 776-77 (E.D. Mich. 2013); *In re Smartphone Geolocation Data Application*, 977 F.Sup.2d 129, 144-45 (E.D.N.Y. 2013) (reiterating the importance of the temporal length of the historical CSLI request); *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel*., 849 F. Supp. 2d 526, 542-43 (D. Md. 2011) (finding that prolonged surveillance reveals information not attainable during short periods of surveillance); *In re U.S. for an Order Authorizing the Release of historical Cell-Site Info*., 809 F. Supp. 2d 113, 117-20 (E.D.N.Y. 2011) (obtaining CSLI records for 113 days captures enough of the user's location information for a long enough time to depict a detailed and intimate picture of the defendant's movements).

But perhaps of the greatest significance, are the decisions by the New York State Court of Appeals in *Weaver* and *Matter of Cunningham v. New York State Dept. of Labor*. *Weaver* held that 64 days of location surveillance violated Art. 1, § 12 of the New York Constitution. The Court in *Matter of Cunningham v. New York State Dept. of Labor* found that location surveillance for a period of "one month" was impermissible under the New York Constitution. In fact, as previously noted, the Court in that case went on to hold that the People's argument that the "workplace" exception to the warrant requirement made the evidence admissible had to be rejected, because obtaining location data on an individual for a period of 30 days was a search that was so inherently "unreasonable" - and the exception only applied to "reasonable" searches – that suppression was constitutionally mandated. *Matter of Cunningham v. New York State Dept. of Labor,* 21 N.Y. 3d at 520-523.

Distilling the holdings of these various decisions, it is fair to say that while the acquisition of a very brief period of CSLI data may be permissible under the diluted standard of a Section 2703(d) order,[15] the six and a half month period of CSLI that was acquired by the People in this case was unquestionably a violation of the Fourth Amendment, Art. 1, § 12 of the New York Constitution and Section 8 of the New York Civil Rights Law.

Another constitutionally significant dynamic that is effected by the length of time that the government conducts location tracking surveillance (and correspondingly, the relative magnitude of the invasion of privacy that results therefrom), is how that element of the Fourth Amendment equation effects other elements. That is to say, as this Court may recall, in *United States v. Davis*, 754 F.3d 1205 (11 Cir. 2014) a panel of the 11th Circuit Court of Appeals held that in order to obtain historical CSLI, a warrant was necessary. Further, that same panel found that the Third Party Disclosure doctrine did not override the Defendant's reasonable expectation of privacy. *Id*. at 1217. The 11th Circuit however vacated its original opinion and sitting *en banc* held that – and principally on the basis of the application of the Third Party Disclosure doctrine – no constitutional violation had occurred. *United States v. Davis*, 2015 U.S. App. LEXIS 7385 (11th Cir. 2015). What is interesting about the Court's *en banc* decision however - and in particular Judge Rosenbaum's concurring opinion (*Id*. at 68-93, Rosenbaum, J. concurring) - is his explanation that "third-party doctrine must be subordinate to expectations of privacy that society has historically recognized as reasonable." *Id*. at 78. Judge Rosenbaum went on to note that: *"[I]n my opinion, the longer-term GPS issue necessarily means that the Dissent is correct in its concerns that the*

[15] *United States v. Shah*, 2015 U.S. Dist. LEXIS 826, 13-14 (E.D.N.C. 2015): "Legislative history behind section 2703(d) states that the standard used for such orders is "higher than a subpoena, but not a probable cause warrant.' Senate Report No. 103-402, at 31 (1994); H.R. Rep. No. 103-827, pt. 1 at 31 (1994)."

expectation of privacy that is infringed by longer-term GPS monitoring may, at some point, become the same expectation of privacy implicated by more and more precise cell-site location technology. When that happens, the historical reasonable expectation of privacy in not being subjected to longer-term surveillance may well supersede the third-party doctrine's applicability to information entrusted to third parties as it pertains to cell-site location information." *Id*. at 87, (emphasis supplied). Accord: *In re United States for an Order Authorizing the Release of Historical Cell-Site Info*., 809 F. Supp. 2d 113 (E.D.N.Y. 2011): "Second, the court concludes that established normative privacy considerations support the conclusion that the reasonable expectation of privacy is preserved here, despite the fact that cell-site-location records is disclosed to cell-phone service providers. Applying the third-party-disclosure doctrine to cumulative cell-site-location records would permit governmental intrusion into information which is objectively recognized as highly private. See *Maynard*, 615 F.3d at 555. Following the decision in *Maynard*, this court concludes that cumulative cell-site-location records implicate sufficiently serious protected privacy concerns that an exception to the third-party-disclosure doctrine should apply to them, as it does to content, to prohibit undue governmental intrusion. Consequently, the court concludes that an exception to the third-party-disclosure doctrine applies here because cell-phone users have a reasonable expectation of privacy in cumulative cell-site-location records, despite the fact that those records are collected and stored by a third party." *Id.* at 126: Also see, *Klayman v. Obama*, 957 F. Supp. 2d 1, 32 (D. D.C. 2013); Alexander Galicki, *The End Of Smith V. Maryland?: The NSA's Bulk Telephony Metadata Program And The Fourth Amendment In The Cyber Age*, 52 Am. Crim. L. Rev. 375, 406-407 (2015).

Judge Rosenbaum ultimately concluded that because the cell site location data in *Davis* was obtained in an urban area where the relative location accuracy was not - in his view – very

precise, that the third party disclosure doctrine trumped Davis' expectation of privacy. Of course in the present case – applying Judge Rosenbaum's reasoning, the result would be opposite for at least two reasons. First, in the instant case, the location data was very precise. (see *amici* brief at pp. 10-18), because the tracking took place in New York City where, given the rather extraordinary proliferation of cell towers, the precision of the location tracking is far, far more accurate. Second – and for the reasons explained above - the amount of historical CSLI that was acquired in this case (201 days, revealing 10,438 separate location points, *amici* brief at p. 1) necessarily would constitute the kind of "long-term" "dragnet" surveillance that Judge Rosenbaum asserts would elevate the expectation of location privacy element over the third party disclosure doctrine. *Id.* at 85-89.

And with regard to the normative inquiry demanded by the second prong of the *Katz* test - i.e. does society objectively accept that a person is entitled to an expectation of privacy in long term historical cell site location information - while resolution of that question is a somewhat indefinite undertaking, there are sources and data available that may provide some guidance to the Court in formulating its conclusions on this issue. For example, in an ongoing survey being conducted by MSNBC, the question was posed: "Should police need a warrant to track cell phone data?" - a full 55% said, yes, 20% said that "it depends on the case," and only one quarter or 25% said that "cell phone owners consent to revealing that data."[16] In a separate survey conducted by the PEW Research Center[17] the results showed that 74% of Americans want to control their

[16] MSNBC, *Should Police Need A Warrant To Track Cell Phone Location Data?* http://www.msnbc.com/msnbc/poll- should-police-need-warrant-track-cell-phone-location-data.

[17] Pew Research Ctr, What Americans Think About NSA Surveillance, National Security And Privacy, May 29, 2015 http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/.

personal information, but few feel like they are able to. Most say it is important to control who can get their information (93%), as well as what information about them is collected (90%). In another poll,[18] nine out of ten voters in the United States want the right to delete links to personal information. "In an AP poll, nearly 60 percent of Americans said they oppose the NSA collecting data about their telephone and Internet usage. In another national poll by the Washington Post and ABC News, 74 percent of respondents said the NSA's spying intrudes on their privacy rights."[19]

Yet another yardstick that may be used to measure the strength of society's views on whether a person's historical cell site and location data should be entitled to a reasonable expectation of privacy, is to take note of the fact that a number of states have passed legislation specifically requiring that a judicial warrant must be secured in order for law enforcement officials to obtain location information. See, Colo. Rev. Stat. Ann. § 16-3-303.5(2) (requiring warrant to obtain cell site data); 16 Me. Rev. Stat. § 648 (same); Minn. Stat. Ann. §§ 626A. 28(3)(d), 626A.42(2) (same); Mont. Code Ann. § 46-5-110(1)(a) (same); Utah Code Ann. § 77-23c-102(1)(a) (same).

It would certainly seem that Justice Kagan believes that a person has a reasonable expectation of privacy in his locations and movements over time. In an almost amusing exchange between Justice Kagan and Deputy Solicitor General Michael Dreeben - during oral argument in *Jones* - Justice Kagan, in her inimitable style, made that point rather clearly:

> MR. DREEBEN: Mr. Chief Justice, advancing technology cuts in two directions. Technological advances can make the police more efficient at what they do through

[18] Beyond the Beltway, Benenson Strategy Group, 2015, http://na-aba.marketo.com/rs/benensonstrategygroup/images/Beyond%20the%20Beltway%20February%202015%20 for%20Public%20Release%5B1%5D.pdf

[19] Update: Polls Continue to Show Majority of Americans Against NSA Spying, January 22, 2014, https://www.eff.org/deeplinks/2013/10/polls-continue-show-majority-americans-against-nsa-spying.

> some of the examples that were discussed today: Cameras, airplanes, beepers, GPS. At the same time, technology and how it's used can change our expectations of privacy in the ways that Justice Alito was alluding to. Today perhaps GPS can be portrayed as a 1984-type invasion, but as people use GPS in their lives and for other purposes, our expectations of 19 privacy surrounding our location may also change. For that –
>
> JUSTICE KAGAN: Mr. Dreeben, that -- that seems too much to me. *I mean, if you think about this, and you think about a little robotic device following you around hours a day anyplace you go that's not your home, reporting in all your movements to the police, to investigative authorities, the notion that we don't have an expectation of privacy in that, the notion that we don't think that our privacy interests would be violated by this robotic device, I'm – I'm not sure how one can say that.* Transcript at pp. 57-58, emphasis supplied.[20]

As a final observation, it is most respectfully asserted that any argument that might be advanced by the People, that the invasion of privacy caused by GPS tracking or real-time location surveillance is somehow materially different from the invasion of privacy caused by the aggregation of prolonged historical CSLI, is simply without merit. "From a Fourth Amendment perspective, there is no 'material difference' between historical and real-time CSLI, as the acquisition of either type implicates the same reasonable expectations of privacy. The privacy interests that are implicated by government access to this data are not 'meaningfully diminished' by a mere delay in disclosure." Lauren E. Babst, *No More Shortcuts: Protect Cell Site Location Data With A Warrant Requirement*, 21 Mich. Telecomm. Tech. L. Rev. 363, 366 (2015). And, in fact, the "mosaic" of the individual's life, activities, associations, habits, etc., is in many instances far more detailed when it is based upon historical CSLI.

[20] Transcript of Oral Argument *United States v. Jones*, No. 10-1259, at pp. 57-58, November 8, 2011 available at: http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf

Application of the Third Party
Disclosure And/Or Assumption of Risk Doctrines

Presumably the decisive battle in this case will be fought over the question of whether the Defendant had a cognizable and constitutionally protected expectation of privacy in his cell site location history, or whether the Third Party and/or Assumption of Risk doctrines operate to contravene any Fourth Amendment claims that might otherwise obtain.

Many judges and scholars[21] have argued that in present day, it is functionally impossible to socially interact, to participate in commerce, to have associational relationships or to satisfy life's basic needs without exposing one's information to third party entities. As Circuit Judge Rosenbaum, in his concurring opinion in *United States v. Davis*, *supra*, candidly explained: "In our time, unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling." *Id*. at 70. It is interesting that Judge Rosenbaum made specific reference to Justice Harlan's dissent in *Smith*; to wit: "As Justice Marshall aptly explained the problem, under the third-party doctrine, 'unless a

[21] See, Colleen Maher Ernst, *Looking Back to Look Forward: Reexamining the Application of the Third-Party Doc-Trine to Conveyed Papers*, 37 Harv. J.L. & Pub. Pol'y 329, 345 (2014): "The modern third-party doctrine creates an expansive exception to the law's general insistence on warrants. Fourth Amendment scholar Orin Kerr acknowledges the rule's general infamy in the academic world: 'The Third-Party doctrine is the Fourth Amendment rule scholars love to hate. It is the *Lochner* of search and seizure law, widely criticized as profoundly misguided.' At the time the Supreme Court decided *United States v. Miller*, courts did not share the understanding of the relationship between the property-based and expectations-based lines of protection articulated by the majority in *Jones*. Accordingly, the *Miller* Court failed to carry out the requisite inquiry involving examination of the Court's early property-based protection for conveyed papers." Also see, Orin Kerr and Greg Nojeim, The Data Question: Should the Third-Party Records Doctrine Be Revisited? ABA Journal, August 1, 2012, http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/.

person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance.' *Smith*, 442 U.S. at 750, 99 S. Ct. 2577, 2585 (Marshall, J., dissenting)." *Id*. at 71.

As the brief filed by *amici* confirms, virtually every person in America owns - and is functionally in constant contact and use of their cell phones for a myriad or reasons. See also; Brad Leneis, *Mapping A Way Out: Protecting Cellphone Location Information Without Starting Over On The Fourth Amendment*, 50 Am. Crim. L. Rev. 499 (2014): "In the last ten years, a new technology - the cellphone - has penetrated American society. Many Americans no longer talk to one another over hard-wired landline phones - instead, they connect using mobile communications devices. And they connect in a variety of ways: through email, instant messaging, text messaging, and online chat, to name a few. Smartphones with powerful computing abilities have now saturated the market as well. As social media applications, or 'apps,' proliferate, these phones become all-purpose, real-time communications devices - compact glass windows into the lives of those around us. Small wonder we feel such an intense connection to them." *Id*. at 499.

Moreover, as District Court Judge Leon put it in his opinion in *Klayman v. Obama*, *supra*: "[the third party doctrine seeks to] strike[] the balance based in large part on a thirty-four year old Supreme Court precedent, the relevance of which has been eclipsed by technological advances and a cell phone-centric lifestyle heretofore inconceivable." (*Id.* at 119-120) "When do present-day circumstances - the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies - become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now." *Id*. at 31.

As a matter of federal constitutional law, the issue may ultimately precipitate down to two competing positions. Either one accepts the proposition that present day society is so manifestly different than it was in the 1970's (when *Miller* and *Smith* were decided) that it is no longer a constitutionally valid premise to assert that the citizenry does not have a subjective, and objectively reasonable, expectation of privacy in information simply because it is processed by third party cell phone providers. Or, alternatively, one takes up the position that anything revealed to a third party is automatically divested of Fourth Amendment protection – and in so doing - accepts the Hobson's choice offered by the majority in the *en banc* decision in *United States v. Davis* that: "If a telephone caller does not want to reveal dialed numbers to the telephone company, he has another option: don't place a call. If a cell phone user does not want to reveal his location to a cellular carrier, he also has another option: turn off the cell phone. *United States v. Davis, supra*, at 57 (Pryor, J., concurring). Cf., *Tracy v. Florida, supra* at 523: "It is true that a cell phone user can prevent locational signals from being used for tracking purposes by turning off the cell phone, thus concealing the signals and the location of the user. However, we do not find that such concealment is a necessary predicate to the Fourth Amendment claim… [r]equiring a cell phone user to turn off the cell phone just to assure privacy from governmental intrusion that can reveal a detailed and intimate picture of the user's life places an unreasonable burden on the user to forego necessary use of his cell phone, a device now considered essential by much of the populace."

And, of course, the answer may well be different depending on whether one applies federal or New York State constitutional law. As previously noted, the *Weaver* Court expressly founded its holding on what it felt was the required outcome under Art. 1, § 12 of the New York State Constitution. And, as the jurisprudence of the New York State Court of Appeals confirms, the Court has been far more protective of the rights of this State's citizens when it perceived that their

privacy was being encroached by technological advances in surveillance techniques and devices than have the federal courts. Indeed, as the Court in *Weaver* made it a point to explain: "*We have adopted separate standards 'when doing so best promotes 'predictability and precision in judicial review of search and seizure cases and the protection of the individual rights of our citizens' (citations omitted) What we articulate today may or may not ultimately be a separate standard. If it is, we believe the disparity would be justified. The alternative would be to countenance an enormous unsupervised intrusion by the police agencies of government upon personal privacy and, in this modern age where criminal investigation will increasingly be conducted by sophisticated technological means, the consequent marginalization of the State Constitution and judiciary in matters crucial to safeguarding the privacy of our citizens.*" 12 N.Y. 3d at 445, (emphasis supplied).

The D-Order, Which Required the Production of the Defendant's CSLI for A Period of Six & ½ Months Was, In Effect, the Equivalent of a "General Warrant"

The well-known historical purpose of the Fourth Amendment was to abolish so-called general warrants and writs of assistance; to prevent the type of searches that were conducted by the British - where what was searched and what was seized was left to the unfettered discretion of the constable conducting the search. The Fourth Amendment was designed to introduce the requirement of judicial intervention and supervision. As the Court noted in *In re Cellular Tels*., *supra*, at 7-8: "A general search leaves to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched… [and] provide[s] no judicial check on the determination of the executing officials that the evidence available justified an intrusion… [t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another."

The decision by federal District Court Judge Lawson in *United States v. White, supra*, is one of the few decisions to confront the issue of the Fourth Amendment requirement of warrant specificity in connection with a location tracking search. In *White* the police had information that he was involved in a "drug trafficking organization operating in Detroit … [and that] Jimmy White was the leader… [who] obtained MDMA from Canada and marijuana from Arizona and Alabama… [t]he affidavit also stated that the source contacted White on the target phone to set up controlled purchases" *Id*. at 7.

Law enforcement officers obtained a warrant for "cell site and GPS data." *Id.* at 6. White ultimately moved to suppress the warrant on the grounds that it fail[ed] to establish probable cause for long-term, real-time active tracking of White through his cell phone." *Id*. at 9. The Court noted that "the surveillance in this case took place over an extended time period — continuously for 30 days on two (or three) separate occasions — and followed White into both public and private spaces. *Id*. at 12-13.

Analyzing the circumstances presented under the two part *Katz* test, Judge Lawson found that: "White certainly had a subjective expectation in his movements over time… [a]nd there are several reasons to conclude that society would recognize that privacy interest as legitimate. For one, White's movement into private spaces, including the interior of his own house, touches on privacy interests that lie '[a]t the very core of the Fourth Amendment… [t]he present case involves a garden-variety drug trafficking crime, nothing more. The blanket surveillance of an individual for thirty days at a time cannot equate to a brief detention, however. The 'nature and quality' of an intrusion of that magnitude (in excess of the 'the 4-week mark') tips the balance in favor of the individual; it constitutes a breach of one's reasonable expectation of privacy that requires the state to demonstrate probable cause as a justification for the intrusion." *Id*. at 16 & 20

Having reached the conclusion that the location tracking of White required a warrant, the Court proceeded to determine White's claim that the warrants that had been issued failed because they were "over broad." To wit; "White contends that the warrants are overbroad because they authorize the police to track him everywhere and continuously for 30 days at a time." *Id*. at 24.

The Court concluded that a warrant that permitted the police to track an individual anywhere he traveled must necessarily be over broad because there was no showing that there was probable cause to suspect he would be committing a crime everywhere he went. As the Court explained its reasoning:

> Once again, a search warrant, including a warrant to track a suspect, must "particularly describ[e] the place to be searched." U.S. Const. amend. IV. Thus, when a law enforcement officer is queried by a magistrate as to where he wants to electronically track a suspect's movements, "everywhere" seldom, if ever, will be an acceptable answer. *Id*. at 28
>
> * * *
>
> In this case, the affidavits did not limit the tracking request to a particular place: they contained no information about any specific place that the government anticipated that White might travel. Instead, the government sought power to electronically track White without limitation every place that he traveled. However, there was no showing that would justify an intrusion of that magnitude; there was no probable cause for a blanket, 30-day search. *Id*. at 29.
>
> * * *
>
> The search warrant in this case allowed the police to track White at all times, night and day, on public streets and in private places, and into areas traditionally protected by the Fourth Amendment… [t]he government concedes that it tracked White even when he "was not on public thoroughfares." The warrant contained no minimization requirement… or any other provision that defined "the discretion of the officer executing the warrant." *Id*. at 31.

Comparing the instant case with the facts described in *White*, it is clear that the circumstances of this case present even a more compelling scenario for suppression than those revealed in *White*.

First, in *White*, law enforcement actually obtained a judicial warrant. In support of the warrant application the government proffered confidential informant information that White was the leader of a drug conspiracy that operated in Michigan, Canada, Arizona and Alabama. *Id*. at 7.

Conversely, in the instant case, the People admitted that they didn't even know whether Mr. Moalawi was actually involved in any of the burglaries and conceded to the Court they wanted to the CSLI "so that we may determine whether Ali Moalawi was assisting Ricky Moore in committing the aforementioned burglaries." Moreover, although the People told the Court that they has seen a Blue Volkswagen Jetta in the vicinity of two of the burglaries and suspected that it may have been a car belonging to Mr. Moalawi. The dates of these incidents were specific – March 14th and July 28th 2014. Nevertheless, rather than seeking CSLI for the several days bracketing these two specific dates, the People opted for a "dragnet search" of the Defendant's records for a period in excess of six months.

If the search warrants in *White* were deemed to be so vague and over broad that they failed to pass constitutional muster, *a fortiori*, a court order - issued on the basis of the diluted standards that apply to a D-Orders – which was not only equally over broad but which allowed unconstrained seizure of every item of location information available (without any geographical, temporal or subject matter related restrictions) for a period of over six months, must necessarily violate state and federal constitutional standards.

It is interesting to note that Justice Sotomayor expressed the view – during oral argument in *Jones* - that allowing 24 hour location tracking was the modern day equivalent of issuing a general warrant. As Justice Sotomayor remarked:

> JUSTICE SOTOMAYOR: Tell me what the difference between this and a general warrant is? I mean –
>
> MR. DREEBEN: A general warrant –
>
> JUSTICE SOTOMAYOR: -- what motivated the Fourth Amendment historically was the disapproval, the outrage, that our Founding Fathers experienced with general warrants that permitted police indiscriminately to investigate just on the basis of suspicion, not probable cause, and to invade every possession that the individual had in search of a crime. How is this different –

MR. DREEBEN: A warrant authorizes –

JUSTICE SOTOMAYOR: -- this kind of surveillance where there's no probable cause, there's not even necessarily reasonable suspicion in –
Transcript at p. 20.[22]

The First Amendment Has Also Been Violated
By The Prolonged Location Tracking of Mr. Moalawi

In his dissent in *Smith*, Mr. Justice Marshall leveled a second criticism at the majority when he forecast that the Court's holding would not only violate the Fourth Amendment but that it would jeopardize First Amendment associational freedoms as well. "Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts… [p]ermitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society." *Id*. at 751. Just as the views of Justice Brandeis in his dissent in *Olmstead* would ultimately take root years later in *Katz*, it would similarly appear that the dissenting views of Justice Marshall in *Smith* have taken root in *Jones*. Indeed, Justice Sotomayor would echo the very same concerns expressed by Justice Marshall in *Smith* in her concurring opinion in *Jones*: "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring - by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track - may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" *Jones*, 132 S. Ct. at 956. Also see, *ACLU v. Clapper*, 2015 U.S. App. LEXIS

[22] Transcript of Oral Argument *United States v. Jones*, No. 10-1259, at p. 20, November 8, 2011 available at: http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf.

7531, 85-86 n. 12 (2d Cir. 2015) (Recognizing, without deciding, the First Amendment issue presented by the collection of metadata).

As the Supreme Court held in *NAACP v. State of Ala. ex rel. Patterson*, 357 U.S. 449, 78 S. Ct. 1163 (1958) there is a "vital relationship between freedom to associate and privacy in one's associations." *Id*. at 462. By the aggregation and mining of the data points revealed through long term CSLI the State is able to determine a person's associational relationships, both with respect to his individual associations as well as his association to groups and organizations. For example, in the instant case, analysis of the cumulative location data provided by the CSLI is likely to reveal, among many other things, that Mr. Moalawi is a practicing Muslim. A review of more than one week of data is likely to reveal with greater clarity that he is frequently near mosques at prayer times.

Government surveillance that encroaches upon First Amendment associational freedoms is subject to a "strict scrutiny" standard. To survive strict scrutiny analysis, the government conduct at issue must: (1) serve a compelling governmental interest; (2) be narrowly tailored to achieve that interest; and (3) be the least restrictive means of advancing that interest. See, Andrew Crocker, *Trackers That Make Phone Calls: Considering First Amendment Protection For Location Data*, 26 Harv. J. Law & Tec 619 (2013); Katherine J. Strandburg, *Freedom Of Association In A Networked World: First Amendment Regulation Of Relational Surveillance*, 49 B.C. L. Rev 741 (2008); Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112 (2007).

The Historical CSLI Should Be Suppressed Because the Defendant's Phone Was Monitored From Locations in Which He had a Traditionally Recognized Expectation of Privacy

As explained in the brief submitted by the *amici*, on virtually every one of the 201 days that the People obtained historical CSLI for the Defendant, signals emanating from his phone that were transmitted from within the confines of places where he had a traditionally recognized expectation of privacy – i.e. his home, his fiancée's home, his car, etc. – were monitored and intercepted. Under the holdings of both *United States v. Karo*, *supra*, and *Kyllo v. United States*, *supra*, this is an indisputable violation of the Defendant's Fourth Amendment rights under both the U.S. Constitution as well as Art. 1, § 12 of the Constitution of the State of New York.

The fact that it is a violation of the Fourth Amendment to monitor signals from the Defendant's cell phone when it transmitting from inside a location in which he has a traditionally recognized expectation of privacy, was readily conceded by the government during oral argument in *Jones*. As the transcript shows:

> JUSTICE SOTOMAYOR: You're – you'e now suggesting an answer to Justice Kennedy's question, which is it would be okay to take the computer chip, put it on somebody's overcoat, and follow every citizen everywhere they go indefinitely. So -- under your theory and the theory espoused in your brief, you could monitor and track every person through their cell phone, because today the smartphones emit signals that police 24 can pick up and use to follow someone anywhere they go. Your theory is so long as the -- that all that what is being monitored is the movement of person, of a person, they have no reasonable expectation that their possessions will not be used by you. That's really the bottom line
>
> MR. DREEBEN: I think that –
>
> JUSTICE SOTOMAYOR: -- to track them, to invade their sense of integrity in their choices about who they want to see or use their things. That's really argument you're making.
>
> MR. DREEBEN: Well, Justice Sotomayor, I think that that goes considerably farther than our position in this case, because our position is not that the Court should overrule *United States v. Karo* and permit monitoring within a private residence. That is off limits absent a warrant or exigent circumstances plus probable

> cause. And monitoring an individual through their clothing poses an extremely high likelihood that they will enter a place where they have a reasonable expectation of privacy.
>
> JUSTICE SOTOMAYOR: Cars get parked in a garages. It happened here.
>
> MR. DREEBEN: Yes, but a car that's parked in a garage does not have a reasonable expectation of 24 privacy as to its location. Anyone can observe –
>
> JUSTICE SOTOMAYOR: Neither does the person.
>
> MR. DREEBEN: Well –
>
> JUSTICE SOTOMAYOR: *A person goes home, and their overcoat gets hung on a hanger. What's the difference.*
>
> MR. DREEBEN: *Once the -- once the effect is in the house, under Karo there is an expectation of privacy that cannot be breached without a warrant, and we're not asking the Court to overrule that.* Transcript at pp. 19 – 20,[23] emphasis supplied.

And of course when the police obtain a person's CSLI for a protracted period, they know beyond peradventure that they will capture – among the other data that this type of "dragnet" search will produce (and the reason why CSLI Orders are simply "general warrants") – signals emanating from places where the person who has been tracked had an undisputed expectation of privacy. As noted above, according to Deputy Solicitor General Dreeben, that is clearly a constitutional violation. Accord: *United States v. Karo, supra*, and *Kyllo v. United States*, *supra*.

It Is The Duty Of This Court To Resolve
The Constitutional Case and Controversy Presently Before It

Two arguments that may be proffered by the People in their opposition to the Defendant's motion to suppress the CSLI data in this case are the contentions that; (1) this is a matter best left to be resolved by the New York State Legislature, and/or (2) that in any event, a trial court should

[23] Transcript of Oral Argument *United States v. Jones*, No. 10-1259, at pp. 19-20, November 8, 2011 available at: http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf.

not reach the issue of whether the Third Party/Assumption of Risk doctrines should be (or not be) applied to excuse the failure of the People to obtain a warrant for the CSLI in this case, because that is a matter which is the province of an appellate court.

Addressing the contention that this is a matter best left to the Legislature, the Defendant would bring to the Court's attention the recent remarks of Justice Kagan made during oral argument (on April 28, 2015) in the so-called "same sex marriage" case, *Obergefell v. Hodges*, 14-556. [24] During his presentation, John J. Bursch, Esq., who argued on behalf of the Respondents, sought to convince the Court that the issue of same sex marriage was a matter better left to the respective states' legislatures, rather than a matter for the Court to resolve. As Mr. Brush asserted:

> MR. BURSH: When you enact social change of this magnitude through the Federal courts, it's cutting off that dialogue and it's saying one group gets their definition and the other is maligned as being irrational or filled with animus. *And that's not the way that our democratic process is supposed to work and there are long term harms to our country and to that fundamental liberty interest to govern ourselves*. All the things that this Court talked about in in the *Schuette* decision, if you take away that dynamic, if it's a court imposed definition as opposed to one enacted to the people through the democratic process. Transcript at p. 74, emphasis supplied.

But Justice Kagan's response – which is particularly applicable to the circumstances at bar – was that our form of government is not a "pure democracy," but rather a "constitutional democracy." As Justice Kagan replied:

> JUSTICE KAGAN: Of course I mean, of course, Mr. Bursch, *we don't live in a pure democracy; we live in a constitutional democracy. And the constitutional the Constitution imposes limits on what people can do and this is one of those cases we see them every day where we have to decide what those limits are or whether the Constitution speaks to something and prevents the democratic processes from operating purely independently*; isn't that right? Transcript at. P. 74, emphasis supplied.

[24] Transcript of Oral Argument, *Obergefell v. Hodges*, 14-556, April 28, 2015, at p. 74, http://www.supremecourt.gov/oral_arguments/argument_transcripts/14-556q1_6k47.pdf.

The point, of course, is that in a constitutional democracy, the issue of what is permitted or forbidden under the constitution (whether it be the United States or the New York State Constitutions) is not a matter for the legislative branch, but rather it is a matter exclusively assigned to the domain of the judicial branch. Most respectfully, it would be an abdication of this Court's obligations under the separation of powers doctrine to leave to the legislature resolution of a constitutional case and controversy. The matter has been squarely put before this Court; is it a violation of the federal or state constitutions to obtain long term CSLI without first obtaining a judicial warrant. The Court is bound to resolve that question. If the legislature elects to pass a law directing that a warrant must be obtained (and as indicated several states chosen to do so) that is an entirely different matter from the situation where a court of original jurisdiction is called upon to resolve a justiciable constitutional case and controversy.

In a parallel context, when the government suggested in *Riley v. California* that the rules regarding information stored in third party servers in the "cloud" should be left to be developed by government law enforcement agencies, Chief Judge Roberts responded by observing, "the Government proposes that law enforcement agencies 'develop protocols to address' concerns raised by cloud computing… [p]robably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols." *Riley v. California,* 134 S. Ct. at 2491.

The other issue that the People may raise in opposition, is the contention that a trial court should not make constitutional determinations of the dimension of whether the Third Party/Assumption of Risk doctrines should (or should not) be applied to non-content data that is emitted from a person's cell phone and is processed and stored by cell phone provider entities - that somehow this is only an issue an appellate court ought to decide. In this regard, the Court's attention is drawn to the observations made by United States Magistrate Judge, Stephen Wm.

Smith of the Southern District of Texas, Houston Division. In a law review article authored by Magistrate Judge Smith he makes some very cogent points about the fact that the courts of original jurisdiction must make these types of decisions and that the courts at *nisi prius* are not only capable, but duty bound to resolve constitutional questions when they are presented. "Magistrate judges swear an oath to uphold the Constitution - the same oath taken by Article III judges"[25] (as well as the Judges of this Court). Magistrate Judge Smith's comments are particular apropos, since they were made in the context of the problems faced in resolving the constitutional questions posed under the Electronic Communications Privacy Act of 1986 (18 U.S.C. §2510, *et seq*,), which the Stored Communications Act (18 U.S.C.2710, et seq.) is a part thereof.

> One of the biggest holes in the ECPA roof is geolocation monitoring. Like an absentee landlord, Congress has all but ignored this widening breach since the problem first came to its attention in 1994. Occasional bills have been introduced to patch this hole, but none have passed and several now languish in committee. In the meantime, magistrate judges, with no congressional guidance about the governing legal standard, have issued hundreds of thousands of orders giving law enforcement access to cell phone location data. This gap in surveillance law has now persisted for eighteen years.
>
> Consider next the judicial branch, and more specifically the Supreme Court, which after all is the ultimate arbiter of constitutional rights in our system. Has it done much better? The Supreme Court has decided a total of two ECPA cases in the quarter century since that statute was passed, and in the most recent case decided in 2010, *City of Ontario v. Quon*, the Supreme Court expressed the worry that maybe they were moving too fast. "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." And what was the emerging technology they were so hesitant to consider in *Quon*? Pagers. Alphanumeric pagers. The pager's role in society is pretty clear now—nobody has one.
>
> * * *
>
> Almost by default, then, these matters have been left to the lowest limb of the judicial branch: the magistrate judge. Unlike the Supreme Court, magistrate judges don't have the luxury of picking and choosing cases, of waiting until various appellate courts have weighed in with their considered judgment on difficult or

[25] Hon. Stephen Wm. Smith, *Standing Up for Mr. Nesbitt*, 47 U.S.F. L. Rev. 257, 268 (2012) http://lawblog.usfca.edu/lawreview/wp-content/uploads/2014/09/Standing-Up-for-Mr.-Nesbitt.pdf.

> novel issues of law. Magistrate judges are on the front lines, grappling hand to hand with the various, novel, and creative surveillance technologies deployed by law enforcement. [26]

Accordingly, any claim that this Court is without authority to fully adjudicate the case and controversy presently pending, should be rejected out of hand. For examples of trial courts deciding the applicability of Third Party doctrine to CSLI, see: *United States v. Cooper*, 2015 U.S. Dist. LEXIS 25935, *supra* at 16-18; In re *Application of United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d *supra* at 116; *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d *supra* at 319.

This Court Should Grant the Defendant's Motion to Suppress

It is the Defendant's position at bar that the acquisition of 201 days of historical CSLI data was a "search" within the meaning of the Fourth Amendment of the United States Constitution as well as Art. 1, § 12 of the Constitution of the State of New York and Section 8 of the New York Civil Rights Law. Moreover, obtaining six plus months of historical CSLI through the use of a D-Order, rendered 18 U.S.C. §2703(d) unconstitutional as applied. Further, based upon the information known to the People and conveyed to this Court on September 17, 2014, any warrant that might otherwise have issued to seize the Defendant's CSLI data for the protracted period of time covered by this Court's Order, would have been over broad and therefore constitutionally infirm.

[26] *Id.* at 261-262.

CONCLUSION

Accordingly, it is respectfully asserted that an Order of this Court should issue, pursuant to the First, Fourth and Fourteenth Amendments of the United States Constitution, Article 1, Section 12 of the Constitution of the State of New York, Articles 700, and 710 of the CPL, Section 8 of the Civil Rights Law, the decisions in *United States v. Jones,* 565 U.S. ___, 132 S. Ct. 945 (2012); *People v. Weaver,* 12 N.Y.3d 433 (2009) and *Matter of Cunningham v. New York State Dept. of Labor*, 21 N.Y.3d 515 (N.Y. 2013) and the inherent and supervisory powers of this Court; (a) suppressing any and all evidence, and/or statements and/or any derivative fruits thereof obtained as the result of the People's unlawful and unconstitutional acquisition and retention of the Defendant's historical Cell Site Location Information data, and; (b) finding that the search of the Defendant's residence and any alleged statements made by the Defendant are the derivative fruits of the People's unlawful acquisition of the Defendant's CSLI, and; (c) dismissing the instant Indictment upon the grounds that it is based upon illegally seized evidence and/or the derivative fruits thereof, or (d) that an Order issue that a *Dunaway/Mapp* hearing be held and (d) and for such other and additional relief as to this Court may seem just and proper.

Dated: June 14, 2015

Respectfully submitted,

_____

John W. Mitchell, Esq.
Law Offices of John W. Mitchell
Counsel to the Defendant
Ali Moalawi
P.O. Box 163
Bedford, New York 10506
(914) 234-6260
lawofficejwm@gmail.com