UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION
No. 5:15-CR-184-BR-6

UNITED STATES OF AMERICA v. JOHN [redacted] [redacted]	DEFENDANT'S MOTION TO SUPPRESS FRUITS OF WARRANTLESS GPS CELL PHONE TRACKING AND INCORPORATED MEMORANDUM OF LAW

Defendant John [redacted] by and through counsel, moves this Honorable Court to suppress from evidence at trial any information obtained from the real-time GPS location tracking (and other precision location tracking) of Mr. [redacted] cellphones on the ground that this real-time warrantless location tracking over 266 days constituted an unreasonable search in violation of the Fourth Amendment.[1]

This precision location tracking was a search (1) because the police intended it to be a search, (2) because it constituted a trespass to chattels under both the physical intrusion and unauthorized usurpation tests, and (3) because surreptitiously usurping a person's private property and turning that property into a tracking device so the government can monitor the person's every movement down to the 150 foot level or closer for 266 days violates a person's reasonable expectation of privacy. No exception to the warrant requirement applied. And a reasonable officer would have known that this pervasive precision location monitoring required a warrant, particularly under the circumstances in this case. Thus, suppression is warranted.

[1] This motion is different than the motions to suppress in United States v. Bey et al, 5:15-CR-166-BR, [D.E. 125, 126, 134]. Those motions related to the collection of general *historical* cell site location information ("CSLI"). This motion relates to the warrantless *real-time GPS tracking* of a citizen for 266 days. As discussed herein, historical CSLI and GPS tracking are categorically factually distinct, and the law governing the collection of each differs dramatically.

I. INTRODUCTION

> It is in this realm—in which the police pick some person whom they dislike or desire to embarrass that the greatest danger of abuse of power lies.

Justice Jackson, "The Federal Prosecutor," An Address at the Second Annual Conference of United States Attorneys, April 1, 1940 (alterations omitted).

At a time unknown, the Raleigh Police Department allegedly received anonymous letters from an ex-girlfriend of Mr. [redacted] who claimed he imported between 1,000 and 2,000 pounds of marijuana each month.

Based on this anonymous information, on December 3, 2014, the Raleigh Police sought the first of at least 21 separate orders under a standard less than probable cause for "prospective Global Positioning Location (GPS)" for the next 60 days of Mr. [redacted] phone and any "telephones with which [his phone] communicates."

Upon finding "reasonable grounds to believe" that this precision cell phone location information would be "relevant and material to an ongoing criminal investigation," a state court judge signed the order and the surveillance began.

With these orders in hand, the Raleigh Police detectives continuously monitored Mr. [redacted] location within 150 feet or closer over the next 266 days.

No search warrant was obtained for this process. However, at one point, the police attempted to obtain an order from the Federal Court authorizing this prospective cellphone tracking under the same federal statute, but Magistrate Judge Numbers specifically prohibited it. [5:15-MJ-1489-RN] *Under Seal* ("[N]othing in this Order shall permit the FBI to . . . track on a continuous basis the location of the CELL PHONE[.]"). Three days later, the police went back

to the state court judge and obtained a contrary order allowing continuous precision location tracking of the same phones addressed in the Federal Magistrate Judge's Order. The police never again asked a Federal Judge for such an order.

To implement this precision location tracking, the Raleigh Police Department demanded that Mr. [redacted] cellphone providers remotely hack into Mr. [redacted] phones to secretly force the phones to disclose their GPS location to the police every few minutes.

The GPS tracking began at 8:20 p.m. on December 3, 2014. By 12:23 a.m. on December 4, 2014, the GPS tracking began locating Mr. [redacted] within his home. Thus, within roughly four hours of beginning to track Mr. [redacted] the officers had violated his well-established constitutional right to be free from unreasonable searches. Yet the officers continued to monitor his precise location over the next 265 days without once obtaining a warrant.

Using this ability to know his location at all times, the Raleigh Police engaged in a pervasive surveillance effort, monitoring his every move, following him wherever they were able, investigating his every interpersonal interaction, reviewing his every commercial transaction, interviewing his family and friends, obtaining his bank records, reviewing his tax records, reading his text messages, taking pictures of him and his family and friends, learning where he shops, who he dates, what vehicles he drives—uncovering every personal, private detail of his life. Using this illegally obtained information, the officers obtained vehicle tracking orders, search warrants, and ultimately a vague Grand Jury indictment.

Yet, despite virtually or physically witnessing his every interaction over 266 days, the police never once witnessed Mr. [redacted] in possession of any illicit substance, nor did they see him conduct a single drug deal. And the total amount of marijuana seized throughout this nine month, multi-state, joint state and federal investigation would not fill a plastic grocery bag.

II. BACKGROUND[2]

A. Cell Phone Technology and Cell Phone Location Information

Cell phones operate through the use of electronic signals called radio waves. To facilitate cell phone use, cellular service providers maintain a network of radio base stations—also known as cell towers—throughout their coverage areas that contain ("cell sites"). A cell site is a portion of the cell tower containing a wireless antenna, which detects the radio signal emanating from a cell phone and connects the cell phone to the local cellular network or Internet.

In the normal course of business, cell phone companies record the cell site that a phone communicated with at the beginning and end of each call. And some cell phone service providers also record the cell site that a phone connected with to send or receive text messages.

Recording the cell site that a phone communicated with facilitates cell phone use by, for example, allowing the cell phone provider to route calls to the phone more quickly. Longer wait times upon making a phone call are indicative of the cell phone provider searching its network to locate a cell tower in range of particular phone. This will occur, for example, when the cell phone has moved a long distance between making or receiving phone calls.

The records of which cell sites a phone communicated with during cell phone use are generally referred to as "cell site location information" ("CSLI"). Because a cell phone typically—although not always—connects to the cell site closet to the cell phone's location, CSLI can be used to broadly estimate where a cell phone may have been at the beginning and

[2] Unless otherwise noted, the source for the information in this section is Exhibit 1, a Declaration of Cell Phone Expert Larry E. Daniel.

end of each cell phone call or other event that generated CSLI. See e.g., AT&T Amicus Brief at 8 ("The device usually – but not always – communicates with the nearest cell tower.").[3]

For example, if Tower A and Tower B are ten miles apart, a record showing that a cell phone connected to Tower A during a particular call suggests—but does not conclusively prove—that the phone was closer to Tower A than to Tower B during the call, and therefore suggests that the phone was within a five mile (or 8,046 meter) radius of tower A.

In the normal course of business, cell phone service providers record only a small amount of CSLI produced each day. See id. at 12 (noting that periodic "'check ins' or registers with the mobile network[, which provide] further, general information about the user's location . . . is not always stored by the service provider[.]"). Therefore, "historical CSLI"—the CSLI in electronic storage with the cell phone service provider at the time a warrant or order requiring disclosure of CSLI is signed—is generally less robust than "prospective CSLI"—the CSLI gathered by the cell phone service provider after the date of, but pursuant to, an order requiring ongoing production of CSLI. See id.

Most important for this motion is not CSCI, but precision location information. In normal circumstances, cell phone service providers do not attempt to pinpoint the precise location of a cell phone with the important exception of when the user calls 9-1-1.

The precision location information corresponding to 9-1-1 calls is the outgrowth of a rule issued by the Federal Communications Commission (FCC) known as E911 Phase II, which mandates that wireless carriers have the capability to identify the latitude and longitude of a cell phone making a 911 call within a radius of no more 100 meters for 67 percent of calls and 300

[3] Available at https://www.eff.org/files/2014/11/17/att_davis_en_banc_amicus_brief.pdf (last accessed November 17, 2015).

meters for 95 percent of calls for network-based (non-GPS) technologies, and 50 meters for 67 percent of calls and 150 meters for 95 percent of calls for handset-based (GPS) technologies). See 47 C.F.R. 20.18(h) (2011).

The purpose of this rule was to ensure that 911 dispatchers would be able to "dispatch local emergency responder to the correct location and to provide assistance to 911 callers more quickly." FCC Guide "911 Wireless Services."[4] Thus, the E911 service was designed to help cell phone users under the assumption that they want emergency service providers to be able to locate them when they dial 9-1-1.

The FCC's E911 requirement does not mandate how cell phone service providers generate the location information of those who dial 9-1-1; it simply demands that they be able to do so. Thus, cell phone service providers use a number of different techniques to precisely locate cell phones that dial 911.

The two main techniques used by cell phone service providers to collect precision location information are "cell tower triangulation" and "GPS location."

Cell tower triangulation operates by sending electrical signals known as "pings" from multiple separate cell towers to a particular phone. Upon entering the phone, these pings command the phone to respond with a responsive electrical signal. By measuring the delay between the responsive signals received by each tower, the cell phone service provider can estimate with a high degree of accuracy the location of the cell phone. This triangulation process is invisible to the user, but it does require the user's phone to expend additional battery power.

GPS location is similar. The Global Positioning System or "GPS" is a satellite-based utility owned and operated by the United States that provides highly-accurate positioning,

[4] https://www.fcc.gov/guides/wireless-911-services (last accessed November 16, 2015).

navigation, and timing services worldwide to any device equipped with a GPS satellite receiver. GPS satellites broadcast radio signals providing their locations, status, and the precise time from their on-board atomic clocks. A GPS device receives these electronic signals, notes their exact time of arrival, and measures the time it took these signals to travel to calculate the device's distance from each satellite in view. Once a GPS device knows its distance from at least four satellites, it can use geometry to determine its location on Earth in three dimensions. GPS.gov.[5]

GPS accuracy has increased dramatically over the years, and today's accuracy rates show that horizontal GPS location is accurate to between two and four meters 95 percent of the time. FAA.gov.[6]

In the normal course of business, cell phone service providers do not maintain records of the GPS coordinates of their customers' cell phones, but the provider may generate such location data at any time by sending an electrical signal, called a "GPS ping," to the phone which commands the phone to transmit its GPS location data back to the service provider. In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 532-33 (D. Md. 2011). This process is also undetectable to the cellular telephone user, id., but it requires the phone to expend additional battery power.

For all practical purposes, continuously obtaining precision location information is the usurpation of a person's cell phone for the purpose of allowing the government to conduct surveillance on that person. Not surprisingly, then, AT&T informed the 11th Circuit in Davis that police throughout the country "consistently" obtain warrants before forcing cell phone service providers to create and disclose this information. AT&T Brief, supra, at 24.

---

[5] http://www.gps.gov/multimedia/poster/poster-web.pdf (last accessed November 16, 2011)
[6] http://www.nstb.tc.faa.gov/reports/PAN86_0714.pdf#page=22 (last accessed November 16, 2015)

B. The Statutory Framework

a. Historical CSLI

The Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq*., which was enacted in 1986 as Title II of the Electronic Communications Privacy Act ("ECPA"), provides the statutory framework for the disclosure by cell phone providers both of the contents of wire or electronic communications in electronic storage, 18 U.S.C. § 2703(b), and of "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication service]," 18 U.S.C. § 2703(c).

Although AT&T submits that the SCA was not intended to allow the disclosure to the government of any location information, AT&T Brief, supra, at 22-25,[7] a number of courts have held that § 2703(c) allows the police to require disclosure of historical CSLI.[8] § 2703(c) reads:

> (c) Records concerning electronic communication service or remote computing service.—
>
> (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
>
> (A) obtains *a warrant* issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issuing using State warrant procedures) by a court of competent jurisdiction; [or]
>
> (B) obtains *a court order* for such disclosure *under subsection (d)* of this section."

(emphasis added).

---

[7] Available at https://www.eff.org/files/2014/11/17/att_davis_en_banc_amicus_brief.pdf (last accessed November 17, 2015).

[8] Again, "historical CSLI" is CSLI that is in electronic storage with the cell phone service provider at the time that a warrant or order for production of CSLI is signed. For example, a warrant or order requiring disclosure of historical CSLI would indicate that the cell phone company must produce CSLI for the 10 days *prior* to the date of the order.

The police did not seek warrants in this case. Rather, they sought orders under § 2703(d), the requirements for which are as follows:

> (d) Requirements for court order.—
>
> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the government entity offers *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.* In the case of a State governmental authority, such a court order shall not issued if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S.C. § 2703(d) (emphasis added).

The standard set forth in § 2703(d) is less than probable cause. See, e.g., In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), 707 F.3d 283, 287 (4th Cir.2013) ("This is essentially a reasonable suspicion standard."); United States v. Davis, 785 F.3d 498, 505 (11th Cir. 2015) ("[§ 2703(d)'s] statutory standard is less than the probable cause standard for a search warrant"); In re U.S. for Historical Cell Site Data ('Fifth Circuit Opinion'), 724 F.3d 600, 606 (5th Cir. 2013) ("The 'specific and articulable facts' standard is a lesser showing than the probable cause standard that is required by the Fourth Amendment to obtain a warrant."); In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to Gov't ('Third Circuit Opinion'), 620 F.3d 304, 315 (3d Cir. 2010) (§ 2703(d) standard is "less stringent than probable cause").

b. Prospective CSLI

The majority of courts to consider the issue have determined that a warrant is required to obtain prospective CSLI.[9] In re U.S. for an Order Authorizing Monitoring of Geolocation and Cell Site Data, 2006 WL 6217584 *4 (D.D.C. 2006) (noting that the majority rule has long been that prospective cellphone tracking requires a warrant).

The statutory basis for this conclusion is that 18 U.S.C. § 3117, which governs the use of tracking devices, requires a search warrant under Fed. R. Crim. P. 41 before officers can use such a device. Id. That statute defines a tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). Because this definition includes current cell phones—at least when their location is being monitored prospectively—the majority of courts to consider the issue have determined that warrants are required for the government to obtain such prospective CSLI.

Moreover, more CSLI is available prospectively than historically because cell phone service providers do not keep all of the CSLI produced each day. However, more CSLI does not mean more accurate location information, since CSLI only gives a broad and uncertain reading of where a person is—generally in geographical spaces from one to ten square miles.

c. Precision Location Information

When the police require cell phone service providers to create new information that is not created in the regular course of business, this demand cannot fall within the confines of the *Stored* Communications Act because that law does not require cell phone service providers to generate new information about their customers for the purpose of allowing the government to

[9] Prospective CSLI is the CSLI generated by the cell phone service provider after, but produced pursuant to, a warrant or order requiring its disclosure—such as an order that requires a cell phone company to produce CSLI for the *next 3 days* following the issuance of the order.

spy on them. Thus, disclosure to the police of precision location information—such as cell tower triangulation or GPS location—is not authorized by the SCA. See Section III.E.d, infra.

The authority under 18 U.S.C. § 3121 *et seq*. for the issuance of pen registers and trap and trace devices also does not allow for the disclosure to the police of precision location information, since 47 U.S.C. § 1002(a) explicitly prohibits the use of such devices for the purpose of tracking the location of a person. That statute states: ". . . with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . , such call-identifying information shall not include any information that may disclose the physical location of the subscriber[.]" 47 U.S.C. § 1002(a).

Because neither the SCA nor the pen register/trap and trace statutes cover situations where cell phone service providers are required to spend their resources to generate new records about their customers that are unrelated to the provision of cell phone service to the customers, the only statutory authority remotely on point is 18 U.S.C. § 3117. As noted above, this law requires the police to obtain a warrant before utilizing "an electronic or mechanical device which permits the tracking of the movement of a person or object." In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 537 (D. Md. 2011) ("[I]f the government seeks to use a particular cellular telephone as a tracking device to aid in execution of an arrest warrant, the government must obtain a tracking device warrant pursuant to Rule 41(b) and in accord with 18 U.S.C. § 3117.).

Federal Rule of Criminal Procedure 41(e)(2)(C) governs the issuance of warrants for tracking devices. That rule reads:

> (C) *Warrant for a Tracking Device.* A tracking-device warrant must identify the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used. The time must not exceed 45 days

> from the date the warrant was issued. The court may, for good cause, grant one or more extensions for a reasonable period not to exceed 45 days each. The warrant must command the officer to:
>
> (i) complete any installation authorized by the warrant within a specified time no longer than 10 days;
>
> (ii) perform any installation authorized by the warrant during the daytime, unless the judge for good cause expressly authorizes installation at another time; and
>
> (iii) return the warrant to the judge designated in the warrant.

As discussed below, the Fourth Amendment also requires police to obtain a warrant before conducting this precision location tracking. Yet, in this case, the Raleigh Police gathered precision location information over the course of 266 days without obtaining a single warrant.

C. Raleigh Police Applications

On December 3, 2014, Raleigh Police Detective Heckman, filled out the first of at least 21 separate applications to state court judges for orders purportedly pursuant to 18 U.S.C. § 2703(d) for "prospective Global Positioning Location (GPS) . . . for 60 days from the date of th[e] order." This application sought the real-time GPS location of Mr. [redacted] phone and any "telephones with which [his phone] communicates." Exhibit 2 at 5.

Finding that there were "'reasonable grounds' to believe that 'records or other information' will be sought related to [Mr. [redacted] phone] and other telephones, of whatever type, with which [his phone] communicates, and this information is 'relevant and material' and will be of 'material aid' to this ongoing criminal investigation" the state superior court judge signed the order. Id.

Importantly, the order explicitly states that "the 'records and other information' sought pursuant to 18 U.S.C. §2703(d) . . . include[ ] . . . prospective Global Positioning Location (GPS) for the duration of the order [.]" Id.

Thus, despite the use of the term "probable cause" elsewhere, the order makes clear that the precision location information was collected based on a reasonable suspicion standard. In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), 707 F.3d at 287; Davis, 785 F.3d at 505. Each of the subsequent cell phone tracking orders included this language, showing that the GPS location tracking of Mr. [redacted] cell phones was conducted pursuant to a standard less than probable cause.

On April 20, 2015, as one order was about to expire, the Raleigh Police and the Government sought a similar order from Magistrate Judge Numbers. 5:15-MJ-1498-RN. Judge Numbers issued an order on April 21, 2015 that prohibited the continuous location monitoring of Mr. [redacted] phones, stating, "nothing in this Order shall permit the FBI to receive . . . location information other than that transmitted at the beginning and end of particular calls or to place calls to the CELL PHONE repeatedly or otherwise to track on a continuous basis the location of the CELL PHONE when no call is being placed or received." Exhibit 3.

Three days later, on April 24, 2015, Detective Heckman sought and received an order from the state court judge authorizing GPS tracking of the same phones addressed in Magistrate Judge Numbers' April 21, 2015 order. Exhibit 4 at 2, 5. Nothing on the face of the April 24, 2015 state court applications indicates that Detective Heckman informed the state court judge that Magistrate Judge Numbers had signed an order three days before that prohibited the collection of the exact information sought in this order. Despite applying for numerous additional cell phone tracking orders over the course of the investigation, neither the Raleigh Police nor the Government ever sought another cell phone tracking order from a federal judge.

The discovery provided, which appears to be incomplete, reveals that between December 3, 2014 and June 26, 2014, the Raleigh Police Department obtained 22 separate orders

purporting to allow them to track 20 specifically identified phones as well any "other telephones with which [those phones] communicate[]" for 60 days each. For some of these identified phones, like Mr. [redacted] phones, there were repeated requests to extend the period for another 60 days.

All told, the Raleigh Police sought and obtained orders purporting to authorize the tracking of 1440 days' worth of cell phone precision location information for identified phones—and an untold amount of information for any phone that the identified phones communicate with. At the average of four location points per hour, this warrantless tracking potentially resulted in the collection of 138,240 real-time GPS location points of at least 20 identified phones (and millions of location points of phones that those identified phones communicated with). Neither the Raleigh Police nor the Government obtained a single warrant authorizing this extraordinary fishing expedition.

III. DISCUSSION

The precision location tracking of Mr. [redacted] cellphones over 266 days constitutes a search under the police intent test, the trespass tests, and the reasonable expectation of privacy test. Warrantless searches are per se unreasonable unless an exception to the warrant requirement applies, and no exception applies here. Therefore, this warrantless precision location by the Raleigh Police violated the Fourth Amendment.

The good faith exception to the exclusionary rule should not apply (1) because the officers engaged in substantially culpable conduct in obtaining these state court orders in violation of an order of the Federal Court; (2) because any reasonable officer would have known that monitoring the location of a person within their home without a warrant violates the Fourth Amendment; (3) because a reasonable officer would have known in light of Jones that

monitoring the precise location of a person over 266 days, or even for 60 days, requires a warrant; (4) because the statutes referenced in these tracking orders prohibit this prospective location tracking; (5) because there was no binding appellate precedent allowing this warrantless tracking, and (6) because the state court orders were obviously facially invalid.

Therefore, the Court should suppress any and all information obtained from this warrantless precision location tracking.

A. The officers intended to conduct a search.

A search is an intrusion by the government into the private life of an individual to gather information. See, e.g., Kyllo v. United States, 533 U.S. 27, 40 (2001). That is what the police intended to do when, reportedly based entirely upon anonymous letters, they secretly turned Mr. [redacted] phone into a tracking device. Generally, when the police intend to search for information they are conducting a search under the Fourth Amendment. Cf. Epperson, 454 F.2d 769, 770 (4th Cir. 1972), cert. denied, 404 U.S. 947 (1972) (holding that because "[searching] is the very purpose and function of a magnetometer," its use is a search under the Fourth Amendment).

In a few carefully limited circumstances, certain seemingly private information is deemed unprotected by the Fourth Amendment; but neither a person's location within their home nor their exact location every few minutes over 266 days falls under those exceptions. Therefore, the Court should deem this tracking what the police intended it to be, a search.

B. The prospective location tracking of Mr. [redacted] cellphones constituted a trespassory search.

The Fourth Amendment protects peoples' "effects," their personal property such as cellphones, from trespasses by the government for the purpose of gathering information. E.g., United States v. Jones, 132 S.Ct. 950 (2012); In re Application for Tel. Info. Needed for a Criminal Investigation, No. 15XR90304HRL1LHK, 2015 WL 4594558, at *6 (N.D. Cal. July 29, 2015) ("Cell phones plainly qualify as 'effects' under the meaning of the Fourth Amendment.").

Trespasses occur through unlicensed physical intrusions upon such property as well as through the unauthorized use of a person's property. See Restatement (Second) of Torts § 217 (1965) (defining a trespass to chattels to include "using or intermeddling with a chattel in the possession of another."); Jones, 132 S.Ct. at 958 ("At common law, any unauthorized intrusion on private property was actionable[.]"), 957 n. 2 ("At common law, a suit for trespass to chattels could be maintained if there was a violation of 'the dignitary interest in the inviolability of chattels[.]'") (Alito, J., concurring).

Thus, any "unlicensed physical intrusion" for the purpose of gathering information constitutes a search. E.g., Florida v. Jardines, 133 S.Ct. 1409, 1415 (2013); Jones, 132 S.Ct. at 949-54; United States v. Silverman, 365 U.S. 505, 506-512 (1961) (holding that any surveillance by the government accomplished by any physical intrusion, "even a fraction of an inch," into a constitutionally protected area constitutes a search); Clinton v. Virginia, 377 U.S. 158 (1964) (per curiam) (where Supreme Court, without comment and by citing Silverman, reversed the conviction of a defendant on facts similar to those in Silverman except that the microphone was placed in the wall rather than through the party wall).

A search also occurs whenever the government "usurp[s] [a person's] property for the purpose of conducting surveillance on him. Jones, 132 S.Ct. at 954 (Sotomayor, J., concurring) (citing Silverman, 365 U.S. at 511-512) (explaining that when the police usurp a person's private property to surveil that person, "[the Government] invad[es] privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection").

Thus, longstanding Fourth Amendment case law illustrates that any unlicensed physical intrusion upon, or any unauthorized use of, a person's cellphone for the purpose of gathering information constitutes a search. Yet, the Raleigh Police Department both physical intruded upon and usurped Mr. [redacted] phones without authority to accomplish the cell phone tracking that allowed them to develop a case against Mr. [redacted]

a. The GPS tracking of Mr. [redacted] phones involved an unlicensed physical intrusion upon those phones.

The precision location tracking of cellphones in this case was not a passive process. GPS-capable phones do not normally send their GPS location to the cell phone service providers. Exhibit 1 at 3, ¶ 20. And cell phone service providers do not regularly triangulate cell phones. Id. at 1, ¶ 9. Therefore, when desiring to track Mr. [redacted] the police hacked into his cellphone. They did so by demanding that the cellphone carrier send secret and unauthorized "precision location pings"[10] to his phones. These precision location pings are electrical signals sent into the phones at least every 15 minutes that command the phones to disclose to the police their precise location.

[10] As used herein, this term—precision location pings—refers to both GPS pings and cell tower triangulation pings.

Precision location pings are comprised of electrical signals. Electrical signals have mass and thus have physical or tangible substance. Id. at 3, ¶ 28. In fact, numerous courts have held that transmitting electrical signals between devices "is sufficiently 'physical' contact to constitute a trespass to property." America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 452 (E.D.V.A. 1998) (citing CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997)); see also Jones, 132 S.Ct. at 962 (Alito, J., concurring) ("some [courts] have held that even the transmission of electrons that occurs when a communication is sent from one computer to another is enough" to establish a physically intrusive trespass" (citing, e.g., CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. at 1021; Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, n. 6 (1996))); Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 404-405 (2d Cir. 2004) (finding that a trespass to chattels can occur through unauthorized use of a webserver through unauthorized electronic searches).

Anyone who has seen lightning or experienced electrical shock knows the tangibility of electrical signals. Benjamin Franklin designed the lightning rod in order to prevent homes from burning to the ground in lightning storms, thus indicating that our founders understood the tangibility of electricity. Batteries contain physical substances that turn into electrical signals and thus deplete the battery. And Einstein's formulation $E=mc^2$, which means Energy = mass * (speed of light)^2, is a recognition that all energy has mass and is thus tangible or physical.

Therefore, the invasion of Mr. [redacted] phones with electrical signals constitutes a physical invasion of his cell phones. Because these pings were sent into his phones without his knowledge or consent, these physical intrusions were unlicensed and therefore constituted a trespass by police for the purpose of allowing the police to surreptitiously gather information about Mr. [redacted] every move. Thus, like the surreptitious information gathering in

Silverman, Clinton, Jones and Jardines, this precision location tracking of Mr. [redacted] phones constituted a search.

The Government may point to Justice Scalia's *obiter dicta* in Jones that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis," Jones, 132 S.Ct. at 935, to argue that the Supreme Court rejected the argument that electronic trespasses can meet the physical intrusion test. This claim should be rejected for the following four reasons.

First, electronic trespasses were not at issue in Jones, so the Court had no occasion to consider the science and case law that establishes that electrical signals are sufficiently tangible to constitute a physical intrusion.

Second, there are a number of situations in which the transmission of electrical signals can occur without a trespass, such as where the police intercept electrical signals or capture electrical signals after they have left a constitutionally protected area or device. See, e.g., Kyllo, 533 U.S. at 34.

Third, there is no indication that the Court did not expect to be taken seriously when repeatedly holding that *any* physical intrusion, no matter how slight, for the purpose of gathering information constitutes a search. See Silverman, Clinton, Jones and Jardines. Those holdings make it immaterial for the Fourth Amendment physical intrusion analysis that the mass of the electrical signals that invaded Mr. [redacted] phone is slight.

Fourth, the Fourth Circuit has held that invading a piece of property with electrical signals is a search on at least two occasions. For example, in United States v. Haynie, the Fourth Circuit stated, "it is clear that the officer's examination of [a] briefcase by means of an X-ray scanner was a search within the meaning of the Fourth Amendment." 637 F.2d 227, 230 (4th

Cir. 1980). Similarly, in United States v. Epperson, the Fourth Circuit held that scanning a person's body with a magnetometer constituted a search. 454 F.2d at 770.

In sum, because electrical signals have mass, they have been found by other courts and should be found by this court to be capable of physically intruding upon property. The precision location pings that allowed the police to track Mr. [redacted] phone over the course of 266 days in this case physically intruded upon his constitutionally protected property without his consent. Therefore, this precision location tracking of Mr. [redacted] cell phones constituted a warrantless physically intrusive search in violation of the Fourth Amendment.

b. The GPS tracking constituted unauthorized usurpation of Mr. [redacted] phones for the purpose of surveilling him, and was thus a trespassory search.

Justice Sotomayor explained that whenever the government usurps a person's property for the purpose of conducting surveillance on him, this conduct "invad[es] privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection." Jones, 132 S.Ct. at 945 (Sotomayor, J., concurring) (citing Silverman, 365 U.S. at 511-512). And Justice Alito explained that the majority holding in Jones establishes that a search occurs whenever the police obtain information via a "trespass to chattel." Id. at 957-958 (Alito, J., concurring).

The precision location tracking of Mr. [redacted] phone was a trespass to chattels, not only because it involved an unlicensed physical intrusion, but also because the police usurped his phone without his permission for the purpose of conducting surveillance on him. See id. at 945 (Sotomayor, J., concurring); id. at 957 n. 2 ("At common law, a suit for trespass to chattels could be maintained if there was a violation of 'the dignity interest in the inviolability of chattels[.]");

Restatement (Second) of Torts § 217 (1965) (defining a trespass to chattels to include "using or intermeddling with a chattel in the possession of another.").

Moreover, this trespass harmed Mr. [redacted] since it drained his phones batteries and—assuming he charged his phones at his home—cost him money by requiring him to recharge the phones more often.

Thus, the Raleigh Police not only usurped this man's private property for the purpose of learning his precise location at all times for 266 days; they also made him pay for this surreptitious tracking. This constitutes a trespass to chattels. It was done by the government for the purpose of collecting information. It was therefore a trespassory search.

C. The continuous monitoring of the precise location of Mr. [redacted] phones over 266 consecutive days violated his reasonable expectation of privacy.

First, the GPS tracking of Mr. [redacted] monitored his location within his residence. It therefore violated his reasonable expectation of privacy. United States v. Karo, 468 U.S. 705, 715 (1984) (holding that a warrant is required to monitor a tracking beeper within a residence). The GPS tracking in this case violated the Fourth Amendment within the first few hours of tracking; yet the police failed to get a warrant for another 265 days, during which they repeatedly violated the clear constitutional prohibition on in-home warrantless tracking.

Second, in Jones, five justices concurred in the result and stated that they would hold that continuously tracking the prospective location of a person's vehicle for 28 days constitutes a search because doing so violates a person's reasonable expectation of privacy. Jones, 132 S.Ct. at 964 ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For . . . offenses [such as drug distribution], society's expectation has been that law enforcement agents and others would not—and indeed . . . simply could not—

secretly monitor and catalogue every single movement of an individual's car for a very long period[,] [i]n this case, four weeks[.]") (Alito, J. concurring, in which Ginsburg, Breyer and Kagan joined); id. at 956 ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'") (Sotomayor, J., concurring).

This holding is not surprising given the longstanding Fourth Amendment case law that the courts "must assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," id. at 950, 958 (quoting Kyllo, 533 U.S. at 34), and that the government runs afoul of the Fourth Amendment "when it uses enhanced surveillance techniques not available to the public to 'see' into private areas." In re Application of U.S. for an Order Authorizing Disclosure of Location Information, 849 F. Supp. 2d 526, 540 (D.M.D. 2011) (citing Kyllo, 533 U.S. at 34).

Precisely tracking the location of a person's cellphone is at least as intrusive as tracking a person's vehicle. "Users typically keep their mobile devices with them during the entire day, potentially providing a much more extensive and continuous record of an individual's movements and living patterns than that provided by tracking a vehicle." AT&T Amicus Brief, supra, at 27. Thus, Justice Sotomayor's lament that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of details about her familial, political, professional, religious, and sexual associations," id. at 955, is even more applicable to prospective cellphone tracking than it is to vehicle tracking.

Cellphone tracking reveals additional details about the person's private life that are not part of the "record of a person's public movements," such as where in a particular house or office they are at any given time. This precision location information allows the government to glean

whether the person is sleeping in the guestroom or master bedroom of a house, what time they lie down and when they rise up, which areas of a hospital or doctor's office complex or any other building they are visiting, which movie they are watching in a particular theater, which shops in the mall they may frequent, who they are visiting in a particular apartment complex, what food they like to eat, where they worship, etc.

Thus, GPS cellphone tracking, like the sense-enhancing technology at issue in Kyllo, allows surveillance into private homes and spaces "that could not otherwise have been obtained without a physical 'intrusion into a constitutionally protected area.'" Kyllo, 533 U.S. at 34.

In short, if five justices believed that prospective GPS tracking of a person's vehicle on public roads for 28 days invaded a reasonable expectations of privacy, certainly monitoring a person's every move in public and in private over the course of 266 days must also violate a person's reasonable expectation of privacy.

Therefore, in addition to constituting a trespassory search, the prospective location tracking of Mr. [redacted] cellphone is also a search under the reasonable expectation of privacy test first established in Katz v. United States, 389 U.S. 347 (1967).

D. Because these searches occurred without a warrant, they violated the Fourth Amendment.

"[W]arrantless searches are per se unreasonable under the Fourth Amendment, [absent] a few specifically established and well-delineated exceptions[.]" City of Ontario, Cal. V. Quon, 560 U.S. 746, 760 (2010) (internal quotation marks omitted).

There is virtually unanimous agreement by the courts that obtaining GPS location information and other precision tracking information requires a warrant. Cf. State v. Perry, 776 S.E.2d 528, 534 (N.C. Ct. App. 2015) ("The majority of federal courts which have considered

the issue have concluded that "real-time" location information may only be obtained pursuant to a warrant supported by probable cause." (citing *United States v. Espudo,* 954 F.Supp.2d 1029, 1034–35 (S.D.Cal.2013))); AT&T Brief, supra, at 24 (noting that police throughout the country "consistently" obtain warrants before obtaining GPS or other precision location information).[11]

Moreover, given the similarity between prospective cellphone tracking and prospective vehicle tracking, it is worth noting that numerous courts have determined that a warrant is required for prospective vehicle tracking. For example, in United States v. Sellers, the Fourth Circuit determined that the warrantless installation and monitoring of a GPS tracking device on a vehicle violated the Fourth Amendment. 512 Fed. Appx. 319, 327 (4th Cir. 2013) (unpublished) (Per Curiam). Numerous courts have agreed. See, e.g., United States v. Ford, 2012 WL 5366049 *8 (E.D.T.N October 30, 2012) (concluding that "the traditional warrant requirement is appropriate in GPS cases."); United States v. Smith, 2012 WL 4898625 *4 (D. Nev. October 15, 2012) ("[I]f the [police] were to perform the same warrantless attachment and use of a GPS device today, it would certainly violate the Fourth Amendment protection from illegal searches and seizures."); United States v. Reynolds, 2012 WL 5305183 *3 (W.D.N.Y. October 25, 2012) ("The Supreme Court in Jones held that the Government's attachment of a GPS device on a vehicle and its use to monitor the vehicle's movements constitutes a search . . . requiring a warrant."). And in a number of cases, the Government has conceded that GPS tracking violated the defendant's Fourth Amendment rights. See, e.g., United States v. Tan, 2012 WL 3535887 *1 (E.D. Cal. August 15, 2012) ("It is also undisputed [by the parties] that, in light of Jones, the installation of the GPS without a warrant did not comport with the Fourth Amendment[.]").

[11] Available at https://www.eff.org/files/2014/11/17/att_davis_en_banc_amicus_brief.pdf (last accessed November 17, 2015).

Finally, no concern for officer safety, exigent circumstances, or other rationale supports the warrantless tracking in this case. Cf. United States v. Richard, No. 2:09-002-PMD, Slip op. at 6-8 (D.S.C. Apr. 12, 2012) (holding that no exception to the warrant requirement applies to vehicle GPS tracking), aff'd 523 Fed. Appx. 323 (4th Cir. 2013); United States v. Ford, 2012 WL 5366049 at *8 (same).

Therefore, the warrant requirement applies to the collection of precision location information, and no exception to the warrant requirement applies in this case. Because the police conducted this precision location tracking without a warrant, they blatantly violated the Fourth Amendment.

E. The good faith exception to the exclusionary rule should not apply.

The court should apply the exclusionary rule in this case for at least six reasons.

a. Judge Numbers specifically prohibited this warrantless tracking.

During this investigation, Federal Magistrate Judge Numbers recognized the constitutional and statutory violations inherent in the request to conduct warrantless precision location tracking, and he issued an order specifically prohibiting it on April 21, 2015. Yet, three days after Judge Numbers' issued his order, Detective Heckman sought and obtained a state court order from a state court judge purporting to authorize this illegal warrantless tracking of the same phones referred to in Judge Numbers' Order. Nothing on the face of the orders indicates that Detective Heckman informed the state court judge that a United States Federal Magistrate Judge had denied this request, which was, after all, purportedly based on a federal statute. This manipulative conduct indicates that the deterrent value of the exclusionary rule would be well-served in this case, particularly when this conduct is viewed in conjunction with the other violations detailed below.

b. Reasonable officers know that in-home tracking requires a warrant.

Since the Supreme Court issued Karo in 1984, a reasonable police officer would have known that tracking a person within their home required a warrant. Karo, 468 U.S. at 715. In this case, the police repeatedly tracked Mr. [redacted] within his home. This in-home warrantless location monitoring in violation of the Fourth Amendment first occurred roughly four hours into what would become a 266 consecutive day tracking odyssey.

c. In light of Jones, reasonable officers must know to get a warrant before conducting extensive precision location monitoring.

At least in light of Jones, which was issued long before the tracking in this case began, an objectively reasonable officer would have known that long-term location monitoring requires a warrant. Police departments throughout the country evidently know this, since, according to AT&T, it is the "consistent" police practice throughout the country to obtain warrants prior to conducting such precision location monitoring. See Section III.D, supra.

d. The tracking orders violated the statutory law.

As reflected in Judge Numbers Order, this tracking violated the statutes purportedly relied upon in the applications and orders.

First, the pen register and trap and trace device authority specifically prohibits the police from using such devices to obtain "information that may disclose the physical location of the subscriber[.]" 47 U.S.C. § 1002(a). So no reasonable officer would believe that they could continuously track Mr. [redacted] using the pen register or trap and trace authority listed in the applications.

Second, the Stored Communications Act (18 U.S.C. § 2701 et seq.), allows the collection of subscriber records that are created through a person's normal use of their cellphone; it does

not allow the police to hack into users' cellphones to force those phones to create new records that are unrelated to the provision of cellphone service to the phone. See, e.g., Espudo, 954 F. Supp. 2d at 1036 ("the entire focus of the SCA is to describe the circumstances under which the government can compel disclosure of *existing* communications and transaction records in the hands of third party service providers. Nothing in the SCA contemplates a new form of ongoing surveillance in which-law enforcement uses co-opted service provider facilities." (Emphasis added)).

Moreover, Congress passed the Stored Communications Act in order to prevent, not to allow, such electronic trespasses. Devine v. Kapasi, 729 F. Supp. 2d 1024, 1026 (N.D. Ill. 2010) ("Congress enacted the relevant provision of the SCA, [18 U.S.C.] § 2701, to protect privacy interests in personal and proprietary information from the mounting threat of computer hackers 'deliberately gaining access to, and sometimes tampering with, electronic or wire communications' by means of electronic trespass." (citing S.Rep. No. 99–541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3557.)).

Finally, the police have occasionally advanced an argument known as the "Hybrid Theory" that suggests that, even though the pen register/trap and trace law prohibits the collection of location information, and even though the SCA does not provide a mechanism for the police to obtain this precision location information, somehow the two laws in combination allow this real-time tracking. This tortured logic has been rejected time and again by courts that have found that there is simply no indication that Congress intended to make the pen register/trap and trace law and the SCA together greater than the sum of their parts. See, e.g., Espudo, 954 F. Supp. 2d at 1037-1043; United States v. Powell, 943 F. Supp. 2d 759, 777 (E.D. Mich. 2013) (police cannot "acquire real-time location information under the 'hybrid' theory combining

pen/trap statute and the SCA authorities); In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device, 396 F. Supp. 2d 294, 315-322 (E.D.N.Y. 2005).

e. There is no binding appellate precedent allowing the warrantless precision location monitoring of a person's cell phone.

A review of United States v. Graham shows that the Fourth Circuit has not established any binding precedent allowing warrantless precision location tracking of cell phones. 796 F.3d 332, 345 (4th Cir. 2015), reh'g en banc granted, No. 12-4659 L, 2015 WL 6531272 (4th Cir. Oct. 28, 2015). To the contrary, Graham indicates that such warrantless tracking violates the Fourth Amendment. Id. Similarly, in State v. Perry, the North Carolina Court of Appeals specifically distinguished cases like the instant case from its holding that collecting historical CSLI does not require a warrant. ___, N.C. App. ___, ___, 776 S.E.2d 528, 539 (N.C. App. 2015) ("[L]aw enforcement did not use GPS, 'real-time' information, or 'ping,' track, trace, or otherwise contact Defendant's cell phone."). Thus, the police were not relying on any binding precedent in conducting these warrantless searches.

f. The orders are invalid on their face.

In his application for a state court order to circumvent the limiting language of Magistrate Judge Numbers' order—in addition to seeking the ability to continuously monitor the location of Mr. [redacted] cellphone in violation of Judge Numbers' Order—Detective Heckman asked for and was purportedly granted the ability to request and review the content of Mr. [redacted] text messages for the last 60 days. Exhibit 4 at 2, 6. The Stored Communications Act explicitly prohibits police from obtaining the content of communications such as text messages that are less than 180 days old without a warrant. 18 U.S.C. § 2703(b)(1)(A).

Moreover, the orders purport to allow the precision location tracking for 60 days of not only the target telephone numbers, but also of any "other telephones, of whatever type, with which [the target phone] communicates." Exhibit 2 at 5, 6; Exhibit 4 at 4, 5. Imagine how many people could have been—and may have been—tracked in violation of the Fourth Amendment based on these orders.

No reasonable police officer would have relied on the legality of such absurdly broad orders.

***

Thus, the police officers in this case violated the constitution, an order of a Federal Magistrate Judge, the statutory law, standard police practice throughout the country, and the common sense rule that police cannot engage in warrantless, boundless, intrusive fishing expeditions allowing them to track scores of individuals in private and public for months upon months. In light of these pervasive, repeated and clear violations, we submit that the court cannot find that the officers acted in a good faith attempt to adhere to the United States Constitution.

Finally, since the good faith exception is not available under the North Carolina Constitution, State v. Carter, 322 N.C. 709, 370 S.E.2d 553, 562 (1988), applying it in this case would upset the incentive structure established to protect the public from constitutional violations. State court judges know that, because no good faith exception exists under the North Carolina Constitution, they need be less cautious in granting orders or warrants; their mistakes are harmless to the defendant. But correspondingly, city police officers must be more careful in seeking orders that will be prosecuted in state court because a bad order or warrant could kill the case. On the other hand, federal judges are likely more cautious than state judges in granting

warrants because of the possibility that evidence obtained in violation of the Constitution will be introduced at trial. Thus, if police are allowed to forum shop like they did in this case, joint state and federal investigations threaten to upset the carefully balanced incentive structures established in each of the separate jurisdictions to protect the constitutional rights of United States and North Carolina citizens.

IV. CONCLUSION

This case presents the exact situation the Supreme Court forecast in United States v. Knotts, where advancements in technology allow police to engage in 24-hour surveillance of any citizen without any meaningful judicial oversight. 460 U.S. 276, 283 (1983).

These orders on their face allow 60 days of precision location tracking of any unknown person unlucky enough to communicate with anyone suspected of being involved in a crime. These orders allowed the Raleigh Police to pick out Mr. [redacted] as the man they wanted to get based entirely on an anonymous tip and, using his private property to obtain a birds-eye view of every minute of his life for nearly a year, allowed them to build an entire conspiracy case against him—not based on any of his acts during the period of surveillance—but instead based on records and information the police were only able to obtain through this warrantless 24-hour a day, 266 day dragnet surveillance.

As technology advances, the frightening possibilities will only increase. The police in this case saw all of the stop signs and ignored each one—from violating orders of the federal court to failing to comply with clearly established constitutional and statutory requirements.

Only by suppressing the information obtained through this illegal precision location tracking can the Court ensure that citizens will be safe from such unreasonable government intrusions in the future.

Respectfully submitted, this the 20th day of November, 2015.

CHESHIRE PARKER SCHNEIDER & BRYAN, PLLC

/s/ Elliot S. Abrams
Elliot S. Abrams
N.C. State Bar # 42639
P. O. Box 1029
Raleigh, NC 27602
(919) 833-3114 (TEL)
(919) 832-0739 (FAX)
elliot.abrams@cheshirepark.com

Attorney for Defendant

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on the date shown below he electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send notification of such filing to Assistant United States Attorneys Jonathan Holbrook and Dena King.

This the 20th day of November, 2015.

/s/ Elliot S. Abrams
Elliot S. Abrams