Cleveland State Law Review

Volume 65 | Issue 1 Article 9

3-1-2017

# Game of Phones: The Fourth Amendment Implications of Real-Time Cell Phone Tracking

Cal Cumpstone
*Cleveland-Marshall College of Law*

# GAME OF PHONES: THE FOURTH AMENDMENT IMPLICATIONS OF REAL-TIME CELL PHONE TRACKING

CAL CUMPSTONE*

## ABSTRACT

With the help of technological advancements, law enforcement can now hijack a targeted individual's cell phone to ping and track the phone's exact location, in real time. Based upon previous rulings, this new tracking process has apparently fallen into a "grey area" of Fourth Amendment jurisprudence. However, real-time cell phone tracking should be a search in terms of the Fourth Amendment and, therefore, require a warrant. Real-time cell phone tracking infringes on an individual's reasonable expectation of privacy, violates the trespass doctrine as a trespass to chattels, and violates the *Kyllo* standard by using technology not in general public use to intrude into a constitutionally protected area.

## CONTENTS



* Cleveland-Marshall College of Law, J.D. expected May 2017. Special thanks to Steve Bradley, Mark Marein, and John Martin for all of their guidance and inspiration throughout the entire article writing process. Special thanks also to Sandra Kerber for serving as an excellent writing instructor and all of her help and advice. Finally, special thanks to Matthew Danese and John Breig.



 

## I. INTRODUCTION

Cell phones are everywhere. As a matter of fact, 90% of American adults own a cell phone.[1] The incredible technological advancements that have occurred over the past two decades have allowed cell phones to essentially evolve into handheld computers.[2] These modern cell phones, also known as smart phones, are capable of internet access and have the ability to use almost an infinite amount of applications, ranging from music playing to picture sharing, to real-time driving directions, to match-making for dating purposes.[3] It is universally accepted that the advancement in cell phone technology has greatly benefited society for communication, entertainment, and business purposes, among countless others; however, this advancement in cell phone technology has inadvertently enabled a very real threat to the privacy of every individual who owns and uses a cell phone.[4]

Law enforcement officers can access the location information that is created both by the ongoing communication between cell phones and cell phone towers and by the GPS technology installed in most cell phones.[5] As a consequence, law enforcement can utilize this information to track the location of a specific cell phone or the individual carrying the phone. Furthermore, this tracking can now be done in real time, thereby converting a person's cell phone into a police-operated tracking device.[6]

---

[1] *Mobile Technology Fact Sheet,* PEW RESEARCH CTR., *http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/* (last updated Oct. 2014).

[2] *See generally The 10 Most Popular Apps of 2015,* TIME (Dec. 21, 2015), http://time.com/4156902/most-popular-apps-2015/; Chris Nickson, *Advances in Mobile Phones*, A TECHNOLOGY SOCIETY (Dec. 1, 2015), http://www.atechnologysociety.co.uk/advances-mobile-phones.html; Lisa Eadicicco & Matt Petronzio, *The 10 Most Popular Smartphone Apps in the U.S.*, MASHABLE (Apr. 3, 2014), http://mashable.com/2014/04/03/popular-apps-chart/#ExK1AJ_7.iqj; *5 Major Moments in Cellphone History*, CBC NEWS (Apr. 3, 2013), http://www.cbc.ca/news/technology/5-major-moments-in-cellphone-history-1.1407352; Nick Wingfield, *Despite a Slowdown, Smartphone Advancements Are Still Ahead,* N.Y. TIMES (Sept. 16, 2012), http://www.nytimes.com/2012/09/17/technology/despite-a-slowdown-smartphone-advances-are-still-ahead.html?_r=0; Justin Meyers, *Watch the Incredible 70-Year Evolution of the Cell Phone,* BUSINESS INSIDER (May 6, 2011), http://www.businessinsider.com/complete-visual-history-of-cell-phones-2011-5.

[3] Nickson, *supra* note 2.

[4] *Id.*

[5] *See generally* United States v. Lambis, No. 15cr734, 2016 WL 3870940, 2016 U.S. Dist. LEXIS 90085 (S.D.N.Y. July 12, 2016); United States v. Powell, 943 F. Supp. 2d 759 (E.D. Mich. 2013).

[6] As opposed to historical cell phone location information which allows police to retroactively look at a cell phone's location, determining where a cell phone has been, not where it currently is. *Powell*, 943 F. Supp. 2d at 772.

Real-time cell phone tracking is a highly invasive procedure; it can be conducted without cell phone users having a scintilla of notice that law enforcement is steadily and constantly monitoring their location.[7] People clearly do not buy phones expecting that the government will monitor their every movement with pinpoint precision.[8] Real-time cell phone tracking is a type of government activity that, although perhaps conducted with good intentions, is far too invasive to be allowed without Fourth Amendment protections.

Currently, there is no bright-line rule regarding the constitutionality of real-time tracking of cell phone location information.[9] Some courts have held that real-time cell phone tracking does not implicate the Fourth Amendment and, thus, allow law enforcement officers to access cell phone location information without a warrant supported by probable cause.[10] Other courts have held that law enforcement's real-time tracking of individuals' cell phones does implicate the Fourth Amendment's prohibition against unreasonable search and seizure.[11] The lack of clarity on this issue has given police and law enforcement the ability to both vastly abuse their powers and track the movements of any individual through his or her cell phone.[12]

This Note argues that courts should automatically consider the real-time tracking of cell phone location information as a search under the Fourth Amendment because it violates a person's reasonable expectation of privacy, constitutes a trespass that activates the trespass doctrine, and relies on technology not available to the general public in conducting a search. Part II of this Note addresses the evolution of Fourth Amendment jurisprudence in terms of searches. Part III of this Note describes the technological background of modern cell phone location tracking capabilities and provides the background that is essential to understanding the issue of real-time cell phone tracking. Part IV of this Note briefly introduces how courts have previously addressed the issue of cell phone location tracking. Part V develops the position that real-time cell phone location tracking implicates the Fourth Amendment. This section compares and distinguishes a widely cited Sixth Circuit case that holds real-time cell phone tracking is not a Fourth Amendment search and synthesizes the issue of real-time cell phone tracking with the seminal Fourth Amendment search cases addressed in the background. Part V also explains why, as a bright-line rule, real-time cell phone tracking should be considered a Fourth Amendment search.

---

[7] *See* Matthew Devoy Jones, *The "Orwellian Consequence" of Smartphone Tracking: Why a Warrant Under the Fourth Amendment is Required Prior to Collection of GPS Data from Smartphones*, 62 CLEV. ST. L. REV. 211, 222-23 (2014).

[8] *See* State v. Earls, 70 A.3d 630, 632 (N.J. Sup. Ct. 2013).

[9] *See Powell*, 943 F. Supp. 2d 759. *Contra* United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

[10] *See Skinner,* 690 F.3d at 777.

[11] *See Powell*, 943 F. Supp. 2d at 767; *see also* United States v. Lambis, No. 15cr734, 2016 WL 3870940, 2016 U.S. Dist. LEXIS 90085 at *4 (S.D.N.Y. July 12, 2016).

[12] *See* Jones, *supra* note 7, at 222-23.

## II. SEARCHES—A BRIEF HISTORY OF FOURTH AMENDMENT JURISPRUDENCE

An examination of the text of the Fourth Amendment and the case law that shaped its jurisprudence will provide valuable insight into developing an understanding of the constitutionally based argument that real-time cell phone tracking should be considered a search. The Fourth Amendment protects the American people by providing as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[13]

This section focuses on the first clause of the Fourth Amendment and addresses the issue of what constitutes a search under the Fourth Amendment.[14] The principles that are established and progressed in this section are imperative in guiding the Fourth Amendment's application to the issue of real-time cell phone tracking.

### *A. Fourth Amendment Fossils—The Pre-History of* Olmstead

The American founding fathers had significant experience dealing with the unbridled power of the British government during colonial America.[15] Accordingly, the founders drafted the Fourth Amendment with the goal of protecting the privacy rights of the individual through the establishment of the right to be secure against the government's unreasonable searches and seizures.[16] Historically, when determining whether a government action constituted a search under the Fourth Amendment, courts utilized a property trespass theory.[17]

In *Olmstead v. United States,* the Court considered, for the first time, the implications of technology on Fourth Amendment searches.[18] The *Olmstead* Court

---

[13] U.S. CONST. amend. IV.

[14] The second clause of the Fourth Amendment is of equal importance but will not be addressed in this Note. Essentially, if a government action has been determined to be a search, in terms of the Fourth Amendment, the government must procure a warrant supported by probable cause before conducting the search. If the government fails to procure a warrant for a Fourth Amendment search, its actions are unconstitutional, and the fruits of the unconstitutional search will likely be excluded. *See* Katz v. United States, 389 U.S. 347, 357 (1976); *see also* Wong Sun v. United States, 371 U.S. 471, 484-86 (1963) (discussing the exclusionary rule).

[15] *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).

[16] *See id.*

[17] *Id.*; *see also* Olmstead v. United States, 277 U.S. 438, 457 (1928).

[18] *Olmstead*, 277 U.S. at 455-57; *see also* R. Craig Curtis et al., *Using Technology the Founders Never Dreamed of: Cell Phones as Tracking Devices and the Fourth Amendment*, 4 U. DENV. CRIM. L. REV. 61, 65 (2014). In *Olmstead,* government agents investigating a large scale bootlegging operation tapped the telephone lines connecting to the main office of the

held that a Fourth Amendment search had not been effectuated because the government did not engage in a physical trespass.[19] The *Olmstead* Court's reliance on the trespass doctrine "placed the core value of Fourth Amendment protection on constitutionally protected places,"[20] and the holding essentially confined the Fourth Amendment to searches and seizures of tangible property.[21] The trespass doctrine would remain at the forefront of search and seizure analysis, under the Fourth Amendment, for the next forty years until the Supreme Court's decision in *Katz v. United States*.[22]

## *B.* Katz *and Beyond—Establishing a Reasonable Expectation of Privacy*

The Supreme Court's opinion in *Katz* created a new doctrine that would provide the basis for almost all subsequent Fourth Amendment search analyses and underlies the argument that real-time cell phone tracking should implicate the Fourth Amendment. *Katz* addressed the legality of the government's conduct in recording telephone calls that private individuals made from a public telephone booth.[23] *Katz* maintained that the reach of the Fourth Amendment cannot hinge on whether a physical intrusion occurred and that the trespass doctrine utilized in *Olmstead* no longer controls Fourth Amendment search and seizure analysis.[24] Furthermore, the Court held that "the Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied . . . and thus constituted a search . . . within the meaning of the Fourth Amendment."[25]

Justice Harlan, in expanding upon the majority's holding in his concurring opinion, reasoned that there was a "twofold test" to determine whether a search or seizure is unreasonable under the Fourth Amendment: "first that a person have exhibited an actual (subjective) expectation of privacy, and second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[26] Justice

---

operation as well as several home telephone lines, all without a warrant. The wiretaps were inserted without any physical trespass onto private property. *Olmstead*, 277 U.S. at 455-57.

[19] *Olmstead*, 277 U.S. at 464-65 (comparing a government agent's intercepting and opening of a sealed letter sent in the mail, a clear search of the sender's papers and effects, to the wiretapping of a phone line which is no more a part of a person's house than the highways on which their house is located).

[20] Curtis et al., *supra* note 18, at 65.

[21] Katz v. United States, 389 U.S. 347, 352-53 (1967); *see also Olmstead,* 277 U.S. at 464-66 (establishing that the Amendment itself is confined to the application only of tangible things – persons, places, papers and effects).

[22] Curtis et al., *supra* note 18, at 66.

[23] *Katz*, 389 U.S. at 348-49.

[24] *Id.* at 353. "The premise that property interests control the right of the Government to search and seize has been discredited." *Id.* at 371 (quoting Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 304 (1967)).

[25] *Id.* at 353.

[26] *Id.* at 361 (Harlan, J., concurring).

Harlan further elaborated that an "intrusion" into a constitutionally protected area itself will not be sufficient to equate to a Fourth Amendment search if the person in ownership of the constitutionally protected area does not have a subjective, reasonable expectation of privacy in the area.[27] Both the majority opinion and Justice Harlan's concurrence acted to effectively replace the trespass doctrine and the dispositive test on Fourth Amendment searches.[28] Justice Harlan's twofold test would serve as the basis of analysis for subsequent seminal cases addressing Fourth Amendment search issues.[29]

After *Katz,* the Supreme Court addressed issues of tracking surveillance via technology and their implications on the subjective, reasonable expectation of privacy test in *United States v. Knotts*, *United States v. Karo*, and *United States v. Jones*.[30] In *Knotts*, the Supreme Court established that an individual has no reasonable and subjective expectation of privacy in his or her movements on public roads and highways.[31] *Knotts* created a limitation on the extent of a person's subjective expectation of privacy.[32] The Court examined whether a Fourth Amendment search had been effectuated when petitioner purchased a five-gallon drum of chloroform to which the police attached a tracking device to the drum before the purchase.[33] Government agents tracked the drum in two separate vehicles (after the drum was transferred between the two), using visual surveillance that was supplemented and augmented by the electronic beeper signals, to respondent Knotts' cabin. [34] Furthermore, the Court saw no indication that the police used the beeper to monitor the location of the drum once it was inside Knotts' cabin or in any way that would not have been observable and in the plain view of the cabin from outside. [35] The Court followed the *Katz* test and held that the monitoring of the beeper signals did not violate any "legitimate expectation of privacy" because the surveillance of

---

[27] *Id.* ("Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overhead, for the expectation of privacy under the circumstances would be unreasonable."); *see also* Silverman v. United States, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

[28] Curtis et al., *supra* note 18, at 66.

[29] *Katz*, 389 U.S. at 361.

[30] *See* United States v. Jones, 132 S. Ct. 945 (2012); United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1983); Curtis et al., *supra* note 18, at 67-68; Jones, *supra* note 7, at 218.

[31] *Knotts*, 460 U.S. at 281.

[32] *Id.* at 276. This limitation is applicable but distinguishable in support of the main argument of this article. *See infra* Part V.B.

[33] *Knotts*, 460 U.S. at 277.

[34] *Id.* at 278.

[35] *Id.* at 285.

the transportation of the drum was an operation that the police could have carried out entirely through visual surveillance.[36]

In *Karo*, the facts were virtually identical to *Knotts,* except that the police installed the beeper tracking device on a can of ether that had already been purchased by respondents, and that the beeper tracked the movements of the can inside the residences of the respondents.[37] Here, the Court held that when electronic surveillance provides a government agent with information about the inside of a private residence that would not be available through plain view from beyond the curtilage of the residence, the government engages in a Fourth Amendment search.[38]

The *Karo* Court reasoned that "indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home" and, therefore, should be monitored and checked under the Fourth Amendment.[39] When considered together, *Knotts* and *Karo* provide that "government may use technology that enhances the senses to improve their ability to conduct surveillance in public areas without any restrictions, but to use such technology to search a private space, such as a home," would qualify as a Fourth Amendment search and necessitate the procurement of a warrant based on probable cause.[40] Then, following *Knotts* and *Karo* and their utilizations of the *Katz* test, the Supreme Court decided to revisit the age-old trespass doctrine in its decision of *United States v. Jones*.[41]

In *Jones*, the Supreme Court chose to rely on the trespass doctrine in lieu of the *Katz* test. On its face, it would appear that a reliance on the trespass doctrine would weaken the case for the inclusion of real-time cell phone tracking into the category of searches requiring Fourth Amendment protection; however, analyzing real-time cell phone tracking as a trespass to chattels supports the position adopted by this Note.[42] *Jones* considered whether the long-term tracking of an individual by a GPS tracking device attached to the undercarriage of a vehicle was a search under the Fourth Amendment.[43] A focal point of the legal analysis was the extensive length and comprehensiveness of tracking that the government agents conducted on Jones.[44]

---

[36] *Id.* at 282-85; *see also id.* at 282 ("Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."); *see also id.* at 283 (quoting United States v. Lee, 274 U.S. 559, 563 (1927) (comparing beeper technology to supplement and augment visual surveillance to the use of a searchlight)).

[37] United States v. Karo, 468 U.S. 705 (1984), 708-09 (noting that the beeper also tracked the package within a locked storage locker).

[38] *Id.* at 715 ("Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises.").

[39] *Id.* at 716.

[40] Curtis et al., *supra* note 18, at 68.

[41] 132 S. Ct. 945 (2012).

[42] *See infra* Section V.C.

[43] United States v. Jones, 132 S. Ct. 945, 948 (2012).

[44] *Id.* at 964.

The search included twenty-eight days of tracking, consisting of 2,000 pages of data over a four-week period.[45] However, the majority never addressed whether the length and comprehensiveness of the surveillance equated to a violation of Jones' reasonable, subjective expectation of privacy because it found that the government conducted a Fourth Amendment search when police trespassed upon Jones' property interests.[46] *Jones* found that the government's actions constituted a physical intrusion of property for the purpose of obtaining information and, therefore, was a search under the Fourth Amendment.[47]

The *Jones* majority's reliance on the trespass doctrine did not replace the twofold, subjective and reasonable expectation of privacy test formulated in *Katz*; rather, it supplemented the *Katz* test and provided another prong of analysis.[48] This new approach, incorporating both *Katz* and *Jones*, is the test that courts now apply to modern Fourth Amendment issues.[49]

## III. TECHNOLOGICAL BACKGROUND—EXPLAINING CELLULAR DATA TRACKING

### *A. Cell Site Location Data*

A basic understanding of modern cell phone tracking technology and procedures is necessary to properly appreciate the analysis and conclusion of this Note, as well as the overall connection between the Fourth Amendment and real-time cell phone tracking. Cell phones operate through constant connection and communication with cell towers operated by respective cell phone service providers.[50] As a cell phone moves in location, it continually reaches out to connect with the nearest cell phone tower, providing for a seamless transition in network connection.[51] When a cell phone connects with a cell tower, it transmits its identifying data, unique to the phone itself, to the cell tower.[52] The movements of a cell phone and its simultaneous

---

[45] *Id.* at 948.

[46] *Id.* at 979 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

[47] *Id.*

[48] *Id.* at 950; *see also id.* at 951 ("As Justice Brennan explained in his concurrence in *Knotts*, *Katz* did not erode the principle 'that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.' . . . *Katz* did not narrow the Fourth Amendment's scope.") (internal citations omitted).

[49] Justice Antonin Scalia was the primary force behind the resurgence of the trespass doctrine in *Jones*, so with his death and impending replacement, the Court could once again abandon the trespass doctrine as a basis to Fourth Amendment search analysis.

[50] *In re* Application of U.S. for an Order for Disclosure of Telecomms. Records, 405 F. Supp. 2d 435, 436-37 (S.D.N.Y. 2005).

[51] *Id.* at 437.

[52] Timothy Stapleton, Note, *The Electronic Communications Privacy Act and Cell Location Data: Is the Whole More Than the Sum of Its Parts?*, 73 BROOK. L. REV. 383, 387

connections and data transmission with various cell towers make it possible to calculate a cell phone's location within a range of several blocks to several feet through a process called multilateration.[53] Additionally, cell phone service providers routinely generate "call detail records" that contain accurate location information relating to the location of a specific cell phone as it moves throughout the course of its usage.[54] The information that is conveyed to cell towers, known as cell site location information (CSLI), is vital to the understanding of cell phone tracking, and forms part of the baseline of the cell phone location data that is at the heart of this Note.[55]

### *B. GPS Location Data*

In addition to the CSLI that is gathered through the multilateration process, GPS data created by the GPS locators installed in the majority of smart phones provide another source of location tracking.[56] The GPS, or Global Positioning System, "is a space-based radionavigation utility owned and operated by the United States that provides highly-accurate positioning, navigation, and timing services to any device equipped with a GPS receiver."[57] GPS technology can provide location information capable of achieving accuracy up to several feet and usually not worse than thirty-three feet.[58] Furthermore, GPS data is generally superior in precision and can be provided without the complicated multilateration process required in typical CSLI data.[59]

### *C. Collecting Location Data*

Law enforcement, in its attempts to track the location of cell phones (and their users), have the option of engaging in either retroactive or prospective tracking.[60]

---

(2007). A cell phone's identification data consists of the ten-digit phone number and a thirty-two-digit number that is unique to each individual cell phone. *Id.*

[53] *See id.*; United States v. Powell, 943 F. Supp. 2d 759, 767 n.2 (E.D. Mich. 2013) (stating that multilateration "is often referred to as 'triangulation,' but because the process may involve more or fewer than three cell towers, 'multilateration' is a more accurate term"). Multilateration is the process of comparing the cell phone's signals to and from multiple cell towers to determine the cell phone's precise location. *Id.* at 767.

[54] *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 833 (S.D. Tex. 2010).

[55] *See* United States v. Lambis, No. 15cr734, 2016 WL 3870940, 2016 U.S. Dist. LEXIS 90085, *1-2 (S.D.N.Y. July 12, 2016) (explaining that CSLI is location information derived from pings between cell sites and target cell phones); *In re* Application for Tel. Info. Needed for Crim. Investigation, 119 F. Supp. 3d 1011, 1013 (N.D. Cal. 2015).

[56] *Powell*, 943 F. Supp. 2d at 767*; see also In re* Application of U.S. Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 533 (D. Md. 2011).

[57] *In re* Application of U.S. Authorizing Disclosure of Location Info., 849 F. Supp. 2d at 533.

[58] *Id.*

[59] *Powell,* 943 F. Supp. 2d at 767.

[60] *Id.*

Law enforcement officers can gather cell phone location information retroactively by recovering historical CSLI, previously created and collected CSLI data that provides information on where a specific cell phone *was* at a past date and time.[61] Law enforcement officers can also speed up the tracking process by pinging the target cell phone and engaging in prospective, real-time tracking.[62] This Note focuses entirely on the latter.

Pinging is understood to be the process of electronically signaling a specific cell phone,[63] which in turn triggers a responsive identification transmission from the targeted cell phone.[64] Law enforcement will ping a cell phone with the intention of generating a record[65] that will provide law enforcement officers with the location of the phone either by accessing the device's GPS coordinates[66] or artificially causing the phone to signal the nearest cell tower(s), initiating the multilateration process and triggering a responsive transmission containing the cell phone's location.[67]

Real-time tracking through cell phone pinging is virtually undetectable to the phone owner and, as surveillance goes, is as clandestine as possible.[68] GPS and CSLI tracking through cell phone pinging allows law enforcement agents to collect "continuous, detailed, and . . . real-time location information" for "hours, days, weeks, months and even years" without an iota of indication to the phone owner.[69] It is imperative to note that this high level of intensely detailed tracking allows law enforcement to track not only the specific cell phone, but also the individual who is in possession of the phone. It is as though every individual who carries a cell phone also carries a homing beacon, continuously broadcasting his or her location to law enforcement.

## IV. MODERN CASE LAW: THE MERGING OF CELL PHONE LOCATION DATA COLLECTION AND FOURTH AMENDMENT JURISPRUDENCE

As the usage of cell phones skyrocketed in relation to the smart phone boom in the mid-2000s, law enforcement officers began to take advantage of this new,

---

[61] *See id.* at 769-70.

[62] *Id.* at 767.

[63] Pinging can also mean the periodical registration with nearby cell towers that the cell phone does on its own but for the sake of clarity this meaning will not be utilized or considered throughout this note. *See In re* Application for Tel. Info. Needed for Crim. Investigation, 119 F. Supp. 3d 1011, 1014 (N.D. Cal. 2015).

[64] *Powell*, 943 F. Supp. 2d at 767.

[65] Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact,* 70 MD. L. REV. 681, 704 (2011).

[66] *See In re* Application of U.S. Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 533 (D. Md. 2011).

[67] *Powell*, 943 F. Supp. 2d at 767.

[68] *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d at 534.

[69] Lenese C. Herbert, *Challenging the (Un)constitutionality of Governmental GPS Surveillance*, 26 CRIM. JUST. 34, 34 (2011).

widespread resource to locate targets of investigations.[70] As a result of this new technology, legal issues relating to the access of cell phone location data began to come to light. In cases where the courts have determined the Fourth Amendment has been implicated, the relevant and overarching issue has been whether the government's collection of cell phone location data constituted a privacy intrusion.[71] In the subsequent paragraphs, the cases form the foundation of the issue of cell phone tracking and are instances where the courts either did not extend their analysis all the way into the Fourth Amendment or where the utilized method of cell phone tracking was not real time.

The subsequent cases provide valuable insight into the legal treatment of searches and tracking via cell phone technology, although they do not directly apply to the real-time cell phone tracking Fourth Amendment analysis. One such case distinguishes historical cell site location information from information that police would recover by the use of a pen register under the pen register statute.[72] The government applied for an order authorizing the disclosure of historical cell site location information under the frequently utilized and broad reaching pen register statute, claiming that the location information could be collected because it could be considered "the contents of an electronic communication."[73] The court determined that the requested information was essentially a means to conduct surveillance of a telephone user because the requested cell site location information would reveal a person's location at a specific time.[74] Furthermore, authorization of the disclosure of the location information would essentially grant the government the ability to install a tracking device without the probable cause necessary for a warrant.[75] However, the court did not consider the overarching privacy matters at stake and instead narrowly focused its decision on the specific application presented in the case.[76]

Distinguishing the legal differences between real-time tracking and passive historical tracking provides the foundation for the assertion that real-time cell phone tracking is a Fourth Amendment search. In the same year that the connection was

---

[70] Taylor Martin, *The Evolution of the Smartphone*, POCKETNOW (July 8, 2014), http://pocketnow.com/2014/07/28/the-evolution-of-the-smartphone; *see also* Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[71] Jones, *supra* note 7, at 226 (providing that issues also include "the type of information collected, governmental interest in the search, the length of surveillance, and the criminality of the defendant").

[72] *In re* Application of U.S. for an Order Authorizing the Use of a Pen Register, 384 F. Supp. 2d 562, 563 (E.D.N.Y. 2005).

[73] *Id.* at 563-64.

[74] *Id.* at 564.

[75] *Id.* (noting that authorization of a pen register under the pen register statute does not require the government to obtain a warrant).

[76] United States v. Powell, 943 F. Supp. 2d 759, 770 (E.D. Mich. 2013) (citing *In re* Application of U.S. for an Order Authorizing the Use of a Pen Register, 396 F. Supp. 2d 294, 322-23 (E.D.N.Y. 2005) (reconsidering government's application for cell site location information that was previously denied in *In re* Application of U.S. for an Order Authorizing the Use of a Pen Register, 384 F. Supp. 2d 562)).

made between location tracking and historical cell site data,[77] the court also considered the issue of real-time tracking via cell site location data.[78] Here, the government sought both historical and real-time cell site location information under the pen register statute. The court concluded that real-time, prospective cell site data should be considered a tracking device under Section 3117 of the Electronic Communications Privacy Act (ECPA).[79] Moreover, the court held that because cell site data should be considered a tracking device, none of the other sections of the ECPA, including the pen register section, would allow the government to gather prospective cell site location information without sufficiently meeting the probable cause standard.[80]

The courts further extended this line of reasoning in *United States v. Graham*.[81] In *Graham*, the defendants were initially arrested and charged with firearm violations; however, after further investigations, the defendants were suspected to be involved in separate robberies.[82] In order to discover the previous whereabouts of the defendants for the purpose of determining if they had been present at the locations of the robberies at the times the crimes had been committed, the government applied for an order to have the defendants' cell phone providers disclose the defendants' locations at the times of the robberies through cell site location information.[83] After reviewing the factual circumstances, the court found that a very real legal distinction existed between historical and real-time cell site location data.[84] The court expounded on the analysis in *United States v. Maynard*[85] and stated that historical data is restricted in its scope because of its historical nature; conversely, real-time data provides the government with the specific movements of the suspect as they are

---

[77] *See In re* Application of U.S. for an Order Authorizing the Use of a Pen Register, 384 F. Supp. 2d at 563.

[78] *In re* Application for Pen Register and Trap/Trace Device with Cell-Site Location Authority, 396 F. Supp. 2d 749 (S.D. Tex. 2005).

[79] *Id.* at 757; s*ee also In re* Application of U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info., 2006 WL 2871743, 2006 U.S. Dist. LEXIS 73324, *17-18 (E.D. Wash. 2006) (stating that "real-time tracking effectively converts a cell phone into a tracking device[,]" and therefore, "cell site data communicated from a cell phone does not constitute an 'electronic (or wire) communication' under the statute because cell site location information "does not involve the transfer of a human voice at any point along the path between the cell phone and the cell tower" it is not a "wire communication"). Section 3117 of Title 18 is titled "Mobile tracking devices" and defines, in subsection (b), mobile tracking devices as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117 (2016).

[80] *In re* Application for Pen Register and Trap/Trace Device with Cell-Site Location Authority, 396 F. Supp. 2d at 757-59.

[81] 846 F. Supp. 2d 384 (D. Md. 2012).

[82] *Id.* at 385-86.

[83] *Id.* at 386.

[84] *Id.* at 391.

[85] 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

occurring[86] and allows the police to "discover the totality and pattern of his movements from place to place to place."[87] Furthermore, the court found that the Fourth Amendment was not implicated in the collection of historical data and that it likely would be implicated in a case involving real-time tracking.[88] This distinction allowed the courts to truly distinguish, jurisprudentially, between historical and real-time location tracking.[89] However, despite the progress made by some jurisdictions in support of the Fourth Amendment protection of real-time cell phone tracking, several jurisdictions do not recognize constitutional protections for cell site and GPS information[90] and, therefore, do not require a warrant for such collection.[91] Then, after previous cases had laid the foundation, the issue of real-time cell phone tracking was finally addressed in *United States v. Skinner*.

*Skinner* serves as a cornerstone of Fourth Amendment jurisprudence in relation to real-time cell phone tracking; however, although the holding and rule of law extrapolated from *Skinner* remains extant, it should be construed narrowly and held to its specific facts. In *Skinner*, defendant Skinner was arrested, charged with, and convicted of "conspiracy to distribute and possess with intent to distribute in excess of 1,000 kilograms of marijuana," among other counts.[92] Through an intensive investigation, Drug Enforcement Agency (DEA) agents determined that Skinner was acting as a drug courier for a large scale drug dealer, which required Skinner to drive to Arizona to pick up and pay for the marijuana and then return to Tennessee to deliver the marijuana to James Michael West, the drug dealer.[93] Authorities identified the specific phone numbers used for communications between Skinner and

---

[86] *Graham*, 846 F. Supp. 2d at 391-92.

[87] *Maynard*, 615 F.3d at 558; *see also* United States v. Knotts, 460 U.S. 276, 281 (1983).

[88] *Graham*, 846 F. Supp. 2d at 389; *see also In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (holding that the Fourth Amendment is not implicated in the government's collection of *historical* cell site data); Jones, *supra* note 7, at 224.

[89] *See In re* Application of U.S. for an Order Authorizing Prospective and Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889, 892 (S.D. Tex. 2014) (describing real-time cell phone location tracking as prospective in nature, in the sense that it "seeks the disclosure of records created in the future, after the government's request . . . enabling law enforcement to monitor the cell phone's location contemporaneously in (or near) real time").

[90] United States v. Powell, 943 F. Supp. 2d 759, 771-72 (E.D. Mich. 2013).

[91] When a warrant, supported by probable cause, is not required for the collection of cell phone location information, it is because courts have ruled that cell phone location information falls under various statutes (including the Stored Communications Act) which allow for the access of information by a court order which is obtained through a showing requiring less than probable cause. *See id.*

[92] United States v. Skinner, 690 F.3d 772, 776 (6th Cir. 2012).

[93] *Id.* at 775. DEA agents lawfully intercepted wire communications from phones subscribed to West's name. Through the wiretap, the authorities learned that West was using a drug courier known as "big foot" (Skinner) who would make the trip back and forth between Tennessee and Arizona on West's behalf. The identity of Skinner was not known until DEA agents arrested only who they knew to be "big foot" in Lubbock, Texas; additionally, Skinner carried out his drug courier duties with the assistance of his son, who was also arrested. *Id.*

West through the wiretap and then obtained an order authorizing the phone company to provide location information consisting of real-time cell site information and GPS location data for Skinner's telephone number.[94] For three days, DEA agents pinged Skinner's phone, tracking his location in real time as he left Arizona with the intention to return to Tennessee.[95] After tracking Skinner to Lubbock, Texas, the DEA agents communicated the information to the Lubbock office, which then effectuated an arrest.[96] Skinner challenged the constitutionality of the DEA's real-time cell phone tracking conducted and claimed it was a violation of his reasonable expectation of privacy in the location information transmitted from his phone.[97]

The court disagreed with Skinner and refused to accept that he had a reasonable expectation of privacy in the location information from his cell phone. [98] The court in *Skinner* relied on the holding in *Knotts* to determine that, because Skinner was traveling in an automobile on a public thoroughfare, he had no reasonable expectation of privacy in his movements and information relating to his location.[99] Effectively, the court determined that, although the information obtained by the cell phone location data (including the GPS data) may have assisted in the tracking of Skinner, the same information could have been gathered by visual surveillance.[100] Therefore, the court in *Skinner* concluded the government's collection of real-time location information was not a search under the Fourth Amendment because, under *Knotts*, Skinner had no reasonable expectation of privacy.[101] Although *Skinner* held that the real-time collection of location information obtained through ping data of the defendant's cell phone was not a search under the Fourth Amendment, it has been distinguished by subsequent cases and should not be followed as a general rule regarding the real-time, active tracking of cell phone location.[102]

---

[94] *Id.* at 776.

[95] *Id.* at 780.

[96] *Id.* at 776.

[97] *Id.* at 777.

[98] *Id.*

[99] *Id.* at 778; United States v. Powell, 943 F. Supp. 2d 759, 773 (E.D. Mich. 2013); *see also* United States v. Knotts, 460 U.S. 276, 281 (1983) ("[O]ne has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.").

[100] *Skinner*, 690 F.3d at 778; *see also Powell*, 943 F. Supp. 2d at 771-72.

[101] *Skinner*, 690 F.3d at 781; *Powell*, 943 F. Supp. 2d at 773.

[102] *See generally Powell*, 943 F. Supp. 2d 759; *In re* Application of U.S. for Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011); State v. Earls, 70 A.3d 630 (N.J. Sup. Ct. 2013).

## V. LIMITING *SKINNER* AND ESTABLISHING A NEW BRIGHT-LINE RULE

### *A. Limitations of* Skinner

The *Skinner* holding should not be extrapolated to anything further than its specific facts, as the facts and rulings constrain its application only to parallel instances.[103] The first limitation inherently imposed on future application of *Skinner* by its facts is the duration and comprehensiveness of the collected location information.[104] Justice Alito, in his concurring opinion in *Jones*, stated that there may be situations where police, using otherwise legal methods, comprehensively track an individual's activities and location to the extent that the very comprehensiveness of the tracking is unreasonable under the Fourth Amendment.[105]

If government agents regularly carry out real-time cell phone tracking via pinging, effectively tracking the suspect's exact location as he travels from place to place, it is clearly comprehensive data collection because it is analogous to *Jones.* The conduct is arguably even more intensive than the location information that was obtained by the GPS device affixed to Jones's car.[106] Location information obtained by a GPS device attached to an automobile is strictly limited to the areas where the automobile is located, essentially driveways, garages, parking lots or roads.[107] Comparatively, real-time location information gathered by a cell phone provides location information as to wherever the cell phone is located, an essentially endless

---

[103] *Skinner,* 690 F.3d 772, allows warrantless cell phone location tracking when "the government seeks to track an individual for a short period of time only, with no foreseeable intrusion into protected areas." *Powell*, 945 F. Supp. 2d at 780.

[104] *Skinner*, 690 F.3d at 780 (stating that location information collected only for three days "accords with expectations of privacy"); *Powell*, 943 F. Supp. 2d at 773-74.

[105] United States v. Jones, 132 S. Ct. 945, 963-64 (2012); *Skinner*, 690 F.3d at 781. In *Jones*, the government tracked the suspect by attaching a GPS device to his car and continuously tracking his movements for a span of 28 days. The majority chose to decide the case based on the trespass doctrine, revitalized from Olmstead v. United States, 277 U.S. 438, 457 (1928), instead of analyzing the case through a reasonable expectation of privacy (*Katz*) test. In his concurrence, Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, addressed the issue of a reasonable expectation of privacy and determined that the extreme comprehensiveness and length of the monitoring constituted a Fourth Amendment search. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

[106] *See Jones*, 132 S. Ct. at 948. In her concurrence, Justice Sotomayor described the possible comprehensiveness of a search involving the location information collected by a GPS device attached to a suspect's car and that, even for short-term monitoring, the comprehensiveness could be enough on its own to implicate the Fourth Amendment. Justice Sotomayor stated that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familiar, political, professional, religious and sexual associations." *Id.* at 955 (Sotomayor, J., concurring).

[107] *See* People v. Weaver, 909 N.E.2d 1195, 1203-04 (N.Y. 2009) (stating that data from a GPS device affixed to an automobile could likely disclose "trips 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").

scope of location possibilities.[108] Therefore, because real-time cell phone location tracking is very likely to be considered comprehensive data, if the tracking is carried out longer than the three days the police used to track Skinner's phone, the Fourth Amendment should be implicated.[109]

The second limitation to *Skinner* is that the court utilized an inherently limiting rationale that would result in an inability to extend the holding to cases involving active, real-time location tracking via pinging. The Sixth Circuit explained, "If a tool used to transport contraband gives of a signal that can be tracked for location, certainly the police can track the signal."[110] Furthermore, according to the court, because the data was produced by the cell phone on its own, the access of the data was not an infringement on a reasonable expectation of privacy.[111] Following this rationale limits law enforcement officers to tracking cell phones by strictly passive means, purely tracking the signals emitted by the cell phone.[112] This rationale effectively overlooks all of the instances where law enforcement actually sends a signal to the phone in order to track it; therefore, any instance of active pinging would exclude the application of *Skinner*.[113] Additionally, because the government is actively and purposefully accessing an individual's cell phone via electronic signaling, this type of pinging would be an intrusion upon an individual's reasonable expectation of privacy.[114]

The third glaring limitation to *Skinner* is that the holding only applies to situations where law enforcement agents track a specific cell phone while the user of the phone is traveling on public thoroughfares.[115] *Skinner* relied heavily on the rationale in *Knotts*, determining that when an individual travels on public thoroughfares, the police are able to track him or her through the unenhanced ability of visual observation.[116] Because the DEA would have acquired the same data and results if the agency had tracked Skinner by simply following him in a car, the court rationalized that, just as in *Knotts*, the GPS-enhanced tracking did not violate any

---

[108] In *Knotts*, the Supreme Court rationalized that if the government ever effectuated such comprehensive surveillance protocols, that essentially equated to a twenty-four hour continual surveillance and tracking, that such "dragnet-type law enforcement practices" could likely implicate the Fourth Amendment. United States v. Knotts, 460 U.S. 276, 284 (1983).

[109] *Powell*, 943 F. Supp. 2d at 774.

[110] *Skinner*, 690 F.3d at 777.

[111] *Id.*

[112] *See id.*

[113] *See Powell*, 943 F. Supp. 2d at 767 (explaining that law enforcement can artificially speed up the process of location tracking cell phones by pinging a cell phone, "that is, sending an electronic signal to a target cell phone . . . that triggers an identification [and location] transmission from the phone").

[114] *See In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 583 (D. Md. 2011).

[115] *Skinner*, 690 F.3d at 781; *Powell*, 943 F. Supp. 2d at 774.

[116] *See* United States v. Knotts, 460 U.S. 276, 284-85 (1983); *Skinner*, 690 F.3d at 780.

reasonable expectation of privacy.[117] Therefore, it is inferable that if law enforcement tracks a phone using real-time pinging and is not categorically certain that the government agents perform the tracking only while the phone and phone user are located on public thoroughfares, the surveillance cannot be shielded from Fourth Amendment implications.[118]

### *B. Real-Time Cell Phone Location Tracking Should Be Considered a Fourth Amendment Search Because It Infringes Upon a Person's Reasonable Expectation of Privacy*

Tracking real-time location information from cell phones should be protected by the Fourth Amendment because individuals have a reasonable expectation of privacy in their location when not on public thoroughfares, and cell phone pinging can disclose when an individual is in a constitutionally protected area.[119] Both *Powell* and *Earls* followed the reasoning set forth in *Karo* to determine that although people do not have a reasonable expectation of privacy in their movements on public thoroughfares, they do have a reasonable expectation of privacy in their location within a private residence.[120] Although a warrant is not required for tracking a person's phone while the individual is on public roads, as soon as a "tracked cell phone signaled that it was inside a private residence (or other location protected by the Fourth Amendment),"[121] a warrant would be absolutely necessary because tracking a person's movements within his or her own private home is arguably the penultimate situation deserving of Fourth Amendment protection.[122]

---

[117] *Skinner*, 690 F.3d at 780 ("[T]he monitoring of the location of the contraband-carrying vehicle as it crossed the country is no more of a comprehensively invasive search than if instead the car was identified in Arizona and then tracked visually and the search handed off from one local authority to another as the vehicles progressed. That the officers were able to use less expensive and more efficient means [pinging] to track the vehicles is only to their credit."); s*ee also Knotts*, 460 U.S. at 284-85; United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito. J., concurring) (stating that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable").

[118] *See Powell*, 943 F. Supp. 2d at 774-75.

[119] *Id.* at 775; State v. Earls, 70 A.3d 630 (N.J. Sup. Ct. 2013).

[120] *Powell*, 943 F. Supp. 2d at 775; *Earls*, 70 A.3d at 639; United States v. Karo, 468 U.S. 705, 713 (1984).

[121] *Powell*, 943 F. Supp. 2d at 774 (first citing *Karo*, 468 U.S. at 712-13; then citing Kyllo v. United States, 533 U.S. 27 (2001)).

[122] The text of the Fourth Amendment specifically states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. CONST. amend. IV. "At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." *Kyllo*, 533 U.S. at 31 (citing Silverman v. United States, 365 U.S. 505, 511 (1961)). It can be argued that the very basis for the Fourth Amendment arose out of the need to protect a person's home from warrantless searches that essentially equated to a government sponsored home invasion masquerading as an inspection. *See* Entick v. Carrington (1765) 95 Eng. Rep. 807. "At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free

Following the plain text of the Fourth Amendment, a serious problem arises in virtually every search involving real-time cell phone location tracking that is not held exclusively to public roads. The widespread use of modern cell phones, which are essentially an "indispensable part of modern life," creates an issue where the "historical distinction between public and private areas" are blurred because cell phones can emit signals from both places.[123] Under "virtually any circumstance," it would be impossible for law enforcement officers to *know in advance* whether or not the prospective real-time cell site location data (or GPS data) collected "would come from a protected area."[124]

Cell site location data and GPS data, both the tools of real-time cell phone location tracking, would allow law enforcement agents to extend its tracking into private residences where the expectation of privacy is unassailable.[125] Information disclosing the cell phone's location inside of a private residence is information that only otherwise could be obtained through a physical search of the residence; in other words, "a police officer would have to, in some manner, enter the premises [and conduct a search of the premises] to obtain the information generated by the cell phone."[126] A search in terms of the Fourth Amendment "occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[127] Private residences are places undeniably protected by a reasonable expectation of privacy and, thus, the Fourth Amendment.[128] Therefore, considering the comprehensive nature of cell phone location tracking, tracking cell phone location in real time (CSLI and GPS) into private residences is an infringement on a reasonable expectation of privacy and a search under the Fourth Amendment.[129]

---

of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." *Karo*, 468 U.S. at 714.

[123] *Earls*, 70 A.3d at 652; *see also* Riley v. California, 134 S. Ct. 2473, 2485 (2014) (stating, famously, "[C]ell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy").

[124] *Powell*, 943 F. Supp. 2d at 776; *see also Karo*, 468 U.S. at 718 ("[Law enforcement officers] have no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises."); *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 543 (D. Md. 2011) ("[I]t is highly unlikely—indeed almost unimaginable—that a cell phone would remain within public spaces."); *Earls*, 70 A.3d at 652 ("[L]aw enforcement had no way of knowing in advance whether defendant's cell phone was being monitored in a . . . private space."). *Cf. Kyllo*, 533 U.S. at 38-39 (determining that barring only the thermal imaging of "intimate details" to be impracticable because law enforcement agents couldn't know *in advance* what through-the-wall surveillance would detect).

[125] *See Powell*, 943 F. Supp. 2d at 774-75.

[126] *Id.* at 775.

[127] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[128] *Karo*, 468 U.S. at 714.

[129] *See In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d at 538.

It is crucial to fully appreciate that the real-time tracking of a cell phone not only can provide the location of the individual carrying the phone, but also indisputably tracks the location of the cell phone itself. In most examples of legal analysis dealing with the issue of real-time tracking under the Fourth Amendment, courts restrict their engagement of the issue to whether the real-time tracking intrudes on the phone possessor's reasonable expectation of privacy in his or her location.[130] However, there has been virtually no analysis on whether real-time location tracking violates an individual's reasonable expectation of privacy in the location of his or her own cell phone, which is not held out in public view.

The Fourth Amendment should protect an individual's reasonable expectation of privacy in the location of his or her cell phone. The plain text of the Fourth Amendment provides, in part, that "[t]he right of the people to be secure in their . . . effects, against unreasonable searches and seizures, shall not be violated[.]"[131]The Supreme Court has previously established that cell phones are items that qualify for the protection of the Fourth Amendment.[132] Moreover, the Supreme Court has held on countless occasions that, absent a showing of probable cause, the only way a law enforcement officer can conduct a physical search or frisk of a person[133] is if the law enforcement officer believes, to a degree of reasonable articulable suspicion, the individual is carrying a weapon (for officer safety).[134] In almost every instance, individuals will keep and carry cell phones in locations that are shielded from the plain view of a law enforcement officer, such as pockets or purses. Therefore, when law enforcement officers actively ping and track an individual's cell phone that happens to be located on his or her person, such as in a pocket or a bag, law

---

[130] *See generally* United States v. Skinner, 690 F.3d 772 (6th Cir. 2012); *Powell*, 943 F. Supp. 2d 759; *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526; State v. Earls, 70 A.3d 630 (N.J. Sup. Ct. 2013).

[131] U.S. CONST. amend. IV. Additionally, it is clear that "effects," in terms of the Fourth Amendment, is considered to be personal property. Lyle Denniston, *Argument Preview: Police and Cellphone Privacy*, SCOTUSBLOG (Apr. 25, 2014), http://www.scotusblog.com/2014/04/argument-preview-police-and-cellphone-privacy/.

[132] *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014).

[133] There are several exceptions to the search warrant requirement (search incident to a lawful arrest, plain view, automobile exception, consent, exigent circumstances, and special needs). It is foreseeable that the only exceptions that could apply to a real-time cell phone tracking situation would be the plain view exception, if the police happened to be tracking a person's phone as they carried their phone out in plain view, and the exigent circumstances exception, for situations where police need to track a cell phone for an emergency situation. The thought that law enforcement would try to actively track a cell phone only when it was displayed in plain view is extremely unlikely, but would be arguable if it could be proved that they strictly abided by the guidelines of the plain view doctrine. Tracking of cell phones for emergency circumstances (under exigent circumstances) is generally allowable but is an entirely different issue in itself that will not be addressed in this note. *See* Arizona v. Hicks, 480 U.S. 321 (1987) (announcing the plain view doctrine); Mincey v. Arizona, 437 U.S. 385, 392 (1978) (exploring exigent circumstances).

[134] *See, e.g.*, Florida v. J.L., 529 U.S. 266, 269-70 (2000); Minnesota v. Dickerson, 508 U.S. 366, 374, 376 (1993); Ybarra v. Illinois, 444 U.S. 85, 91 (1979); Terry v. Ohio, 392 U.S. 1, 20-21, 24 (1968).

enforcement has effectively conducted an unconstitutional Fourth Amendment search of the individual's person[135] to determine that the person is, in fact, carrying a cell phone.[136]

People do not purchase cell phones to be utilized as tracking devices against their interests, and this expectation that the government will not commandeer a person's cell phone to track their every movement is a reasonable expectation. For a brief and final argument, for the sake of a Fourth Amendment analysis, note the seminal case of *Katz* and, more specifically, Justice Harlan's immensely influential concurring opinion. In terms of Fourth Amendment analysis, Justice Harlan determined that there was twofold test: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[137] Considering real-time cell phone location tracking, it is understood and accepted that people do not buy cell phones to serve as tracking devices for the police to utilize, nor do people reasonably expect the government to hijack their cell phones to use in that manner.[138]

People purchase and use cell phones to communicate with others and to access the Internet and the myriad applications available to cell phone users, not to share their location information with the police.[139] Cell phone users may be aware that their phones have the capability to transfer and generate location information through the general course of phone usage, but most people are entirely unaware of the extent of modern tracking capabilities and "reasonably do not expect law enforcement to convert their phones into precise, possibly continuous tracking tools."[140] Therefore, real-time cell phone tracking through CSLI and GPS data is an infringement on a reasonable expectation of privacy and constitutes a Fourth Amendment search. In addition to real-time cell phone tracking infringing on a reasonable expectation of privacy, there is also a strong argument that real-time cell phone tracking implicates the Fourth Amendment through the application of the trespass doctrine.

### *C. Real-Time Cell Phone Location Tracking is a Fourth Amendment Search Under the* Jones *Trespass Doctrine Because Government Pinging Private Cell Phones Constitutes a Trespass to Chattels*

The Supreme Court in *Jones* found the extensive GPS tracking of Jones's car to be a Fourth Amendment search, not because it violated the defendant's reasonable

---

[135] Even the crime prevention tactic of stop-and-frisk is strictly based on a police officer having a reasonable suspicion that the person to be stopped and frisked is armed and dangerous. David Rudovsky & Lawrence Rosenthal, *The Constitutionality of Stop-and-Frisk in New York City*, 162 U. PA. L. REV. ONLINE 117 (2013), https://www.pennlawreview.com/online/162-U-Pa-L-Rev-Online-117.pdf.

[136] *See* cases cited *supra* note 130 (arguing that, without applicable exceptions, the search of a person without a warrant is unconstitutional).

[137] Katz v. United States, 389 U.S. 347, 361 (1976) (Harlan, J., concurring).

[138] State v. Earls, 70 A.3d 630, 634-39 (N.J. Sup. Ct. 2013).

[139] *Id.* at 643, 652-53; *see also* Riley v. California, 134 S. Ct. 2473, 2484-85 (2014) (describing, in both cases, the indispensable nature of cell phones in modern life).

[140] *Earls,* 70 A.3d at 651-52.

expectation of privacy, but because the government's conduct constituted a trespass.[141] The Court elaborated that a trespass itself is not sufficient for a Fourth Amendment search; rather, there must be a trespass that is conjoined with "an attempt to find something or to obtain information."[142] However, the issue at hand in *Jones* was not analogous to the issue of real-time cell phone tracking; therefore, the Court did not address the extent of the applicability of the trespass doctrine.[143]

*Skinner* did not truly entertain the applicability of the *Jones* trespass doctrine to the issue of real-time cell phone tracking, but the Court's rationale portrayed a belief that the data accessing process was too passive to be considered a trespass.[144] The *Skinner* Court erred in its understanding and explanation of the process of real-time tracking.[145] The result was a failure both to realize the active nature of the process and to entertain the issue that the government's active electronic interference with an individual's cell phone may be a trespass to chattels, thereby triggering an analysis under the trespass doctrine.[146]

Lower courts have, on several occasions, held that electronic signals are sufficient contact to constitute trespass to chattels.[147] Trespass of chattels has been defined to include the "using or intermeddling with a chattel in the possession of another."[148] The comments to the Restatement tend to confine the tort to instances of physical contact; however, in instances of electronic signals, courts have found that physical contact is not necessary if some harm can be proved.[149] Active signaling by

---

[141] United States v. Jones, 132 S. Ct. 945, 951-53 (2012).

[142] *Id.* at 951 n.5.

[143] The court maintained that instances of government surveillance involving strictly the transmission of electronic signals and not including any trespass would still be subject to a Katz analysis. The Court stressed that the trespass doctrine was not replacing the Katz test; it would strictly be a supplementary tool for Fourth Amendment search analysis. *Id.* at 953.

[144] *See* Case Comment, *Sixth Circuit Holds that "Pinging" a Target's Cell Phone to Obtain GPS Data is Not a Search Subject to the Warrant Requirement*—United States v. Skinner, 126 HARV. L. REV. 802, 806 (2013) (citing United States v. Skinner, 690 F.3d 772, 776 (6th Cir. 2012)).

[145] *Id.* at 806-07. Furthermore, the section of this article explaining the technological approach for attaining real-time cell phone location information demonstrates the active nature of real-time tracking. The *Skinner* court grossly misrepresented the invasive process utilized to attain this private and personal information. *See id.* at 804-06.

[146] *See id.*

[147] *See id.* at 808. Justice Alito's concurrence explicitly raised the relevant question: "Would the sending of a radio signal to activate [a GPS] system constitute a trespass to chattels?" *Jones*, 132 S. Ct. at 962. He then pointed out that lower courts have previously held that electronic signaling has been sufficient to find a trespass to chattels. *Id.*

[148] RESTATEMENT (SECOND) OF TORTS § 217 (AM. LAW INST. 1965).

[149] Case Comment, *supra* note 144, at 807 (citing RESTATEMENT (SECOND) OF TORTS § 217 cmt. e, § 218(b) (AM. LAW INST. 2016)). Also worth noting is that there may be instances where "the intermeddling is actionable even though the physical condition of the chattel is not impaired." RESTATEMENT (SECOND) OF TORTS § 218 cmt. h (AM. LAW INST. 2016). *See also* Case Comment, *supra* note 144, at 807, stating:

law enforcement would cause an individual's phone to do something out of the ordinary and impair the value of the phone in several ways, "including the use of more battery power and a decrease in [a] disposable phone's intended ability to confer greater privacy on the user," among others.[150] The detrimental effects of active signaling would be sufficient for a showing of harm to the chattel to satisfy a finding of trespass.[151] Furthermore, the courts have exhibited a willingness to entertain the ever-evolving state of technology and its application to trespass to chattels to find more ways in which non-physical interferences can constitute a trespass.[152] Although *Jones* did not directly address the trespass implication of electronic signaling and *Skinner* decided not to apply the doctrine, if a court addressed the issue of real-time cell phone tracking as the active and invasive process it is, it would likely find a trespass to chattels and a Fourth Amendment search under the *Jones* trespass doctrine.[153] Finally, in instances where law enforcement uses special technology to conduct real-time cell phone tracking, there is an additional justification that courts should utilize in order to rationalize the implication of the Fourth Amendment.

### *D. Real-Time Cell Phone Location Tracking by Cell Site Simulator Devices Should Be Considered a Fourth Amendment Search Because It Violates the Reliance on Technology Established in* Kyllo

In *Kyllo*, the Supreme Court held that the government's use of a thermal imaging device to develop heat images of the inside of a home constituted a search under the Fourth Amendment.[154] To investigate a marijuana growing operation without

---

In CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997), a federal district court noted that "trespass to chattels has evolved from its original common law application . . . to include the unauthorized use of personal property." Citing cases that had deemed electronic signals to be sufficiently physically tangible, the court held that bulk spam emails sent to the plaintiff's servers caused sufficient harm (in the form of decreased bandwidth and goodwill toward the plaintiff's company) to sustain an action for trespass to chattels. In a later case, the same district court found that the decrease in a server's value as a safe location for files following the defendant's unauthorized access was also sufficient. Similarly, the Second Circuit enjoined a company from installing automatic software updates that, if allowed, could crash plaintiff's computers. Likewise, a federal district court in Illinois held that a defendant's unauthorized spyware installation on the plaintiff's computer created harms such as depleted memory, increased energy and bandwidth usage, elevated internet use charges, domination of on-screen pixels, and increased user frustration, thus supporting a cause of action for trespass to chattels.

[150] Case Comment, *supra* note 144, at 807-08.

[151] *See id.*

[152] *See generally* John D. Saba, Jr., Comment, *Internet Property Rights: E-Trespass*, 33 ST. MARY'S L.J. 367 (2002).

[153] *See generally id.*; Case Comment, *supra* note 144; United States v. Jones, 132 S. Ct. 945 (2012); United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

[154] 533 U.S. 27, 29-30, 34 (2001).

entering a private home, law enforcement used a thermal imaging device to scan the home from the exterior and develop heat images of its interior.[155] Through the emitted heat signatures, law enforcement officers determined that the homeowners were using halide lights to facilitate marijuana growth.[156] In its decision, the Court reasoned that using sense-enhancing technology to obtain information relating to the inside of a home, which is information that could not have been otherwise gained without a "physical intrusion into a constitutionally protected area, constitutes a search—at least where the technology in question is not in general public use."[157] Considering that it is practically impossible for law enforcement officers to know in advance whether or not the prospective real-time cell site location data (or GPS data) collected would come from within a home, it is appropriate to subject the tracking technology to a *Kyllo* analysis.[158]

In many cases, law enforcement utilizes technology known as cell site simulators; these simulators give off signals to deceive cell phones into believing that the device is a cell tower so that the cell phone will transmit its location to the simulator.[159] Cell site simulators work in different ways depending on the specific device being used; two commonly used devices are the TriggerFish and the StingRay.[160] A TriggerFish can intercept a cell phone's information, as well as verbal content of a phone conversation, but the interception can only come from active cell phones as they make calls and actively transmit.[161] StingRays are devices that can capture cell phone information by actively "forcing" the phone to transmit its information by emitting signals that trick cell phones into treating the simulator as if it were a real cell tower.[162] Information collected by either cell site simulator device can effectively be used by law enforcement to triangulate and locate a specific cell phone to a "narrow geographical location."[163] These invasive devices are not utilized by or available to the general public.[164]

---

[155] *Id.* at 29-30.

[156] *Id.*

[157] *Id.* at 34; *see also In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 539 (D. Md. 2011) ("The Supreme Court has maintained a distinction between areas where a person can be publicly viewed and areas that could not be observed 'from the outside' using traditional investigatory techniques.").

[158] United States v. Powell, 943 F. Supp. 2d 759, 776 (E.D. Mich. 2013); *see also In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d at 540 (stating that the government "runs afoul" when it uses enhanced surveillance technology, not available to the public, to search private areas).

[159] Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 185 (2014).

[160] *Id.* at 191.

[161] *Id.*

[162] *Id.* at 191-92.

[163] *Id.* at 193.

[164] *Id.* at 191-93.

The primary manufacturer of cell site simulators is the Harris Corporation, which sells the simulator devices to state and federal law enforcement agencies.[165] Furthermore, the Harris Corporation sells its cell site simulators to the government "from a catalogue that it conceals from the public on national security grounds," doesn't disclose the devices on its website, and warns that usage of the devices outside law enforcement purposes could be a criminal offense, punishable by a term of five years in jail.[166] In fact, one of the only ways an individual can access a device for personal use is to buy high-tech computer equipment and construct a homemade cell site simulator device.[167] The device cannot be considered to be in general public use if the manufacturers of the devices refuse to sell to members of the general public.[168]

The use of cell site simulator devices in real-time cell phone tracking is analogous to the use of the thermal imagining device in *Kyllo*. Just as the government used a thermal imaging device to "look into" Kyllo's home, the government's use of cell site simulators will effectively "look into" the phone possessor's home if the targeted cell phone is inside the home.[169] Similarly, as the thermal imaging device used in *Kyllo* was not a device available to the general public, cell site simulators used in real-time cell phone tracking are also not available to the general public.[170] Therefore, considering that it is a practical impossibility for law enforcement to know in advance whether or not real-time cell phone data will come from within a private, constitutionally protected residence when law enforcement utilizes a cell site simulator device that is clearly not available to the general public, the government effectuates a Fourth Amendment search.[171]

---

[165] *Id.* at 185; Ryan Gallagher, *Meet the Machines that Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/. Oakland County, in Michigan, has recently received a state grant to purchase a newer, higher powered, cell site simulator, also manufactured by Harris Corporation. This device, called a Hailstorm, is significantly more powerful than a StingRay and has previously been used the United States military in anti-terrorism efforts. The Oakland County Sheriff's Office is one of about two dozen forces that utilize this device. The Hailstorm is such a covertly utilized device that "even national experts will only speculate about its capabilities." Joel Kurth & Lauren Abdel-Razzaq, *Military Device Sweeps Activity in Wide Area*, DEMOCRATIC UNDERGROUND (Apr. 5, 2014), http://www.democraticunderground.com/10024787166.

[166] Gallagher, *supra* note 165. Harris Corporation cell simulator devices are "developed for military and spy agencies and information about them is on 'bureaucratic lockdown' because the manufacturer, Harris, claims specifications are a 'trade secret.'" Kurth & Abdel-Razzaq, *supra* note 165.

[167] *See* Owsley, *supra* note 159, at 191. A cell site simulator could be constructed by a bright "computer whiz" with about $1,500 worth of equipment. *Id.*

[168] *See* Gallagher, *supra* note 165.

[169] *See* Kyllo v. United States, 533 U.S. 27, 29-30, 34 (2001); United States v. Powell, 943 F. Supp. 2d 759, 776 (E.D. Mich. 2013).

[170] *See Kyllo*, 533 U.S. at 34; Owsley, *supra* note 159, at 191.

[171] *See Powell*, 943 F. Supp. 2d at 776; United States v. Karo, 468 U.S. 705, 718 (1984) (stating that [law enforcement officers] have "no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises"); *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849

## VI. CONCLUSION

Developments in technology will continue to influence all facets of life, including criminal law and the way law enforcement will attempt to protect social order. However, as technology allows law enforcement to increasingly invade the privacy of U.S. citizens, imposed limitations on the pervasiveness of the government's reach are imperative to the protection of individual liberty and privacy.

Real-time cell phone location tracking should be a Fourth Amendment search as a bright-line rule. Real-time cell phone tracking violates a person's reasonable expectation of privacy in both his or her physical location within constitutionally protected areas, such as homes, and in the location of the cell phone itself when held in pockets or containers not in open view of the general public. Furthermore, individuals do not purchase cell phones with the expectation that the government will hijack the cell phone and use it as a tracking device, evidencing a reasonable expectation of privacy. Real-time cell phone tracking constitutes a trespass to chattels and thereby implicates the once defunct trespass doctrine revitalized in *Jones*. Finally, the use of cell site simulators in conducting real-time cell phone tracking equates to the use of technology, not available to the general public, to facilitate a search, which is conduct that *Kyllo* held unconstitutional under the Fourth Amendment. To continue to uphold the Fourth Amendment and truly protect the people from unreasonable searches, the Fourth Amendment must apply to the highly invasive and comprehensive government conduct that is real-time cell phone location tracking.

F. Supp. 2d 526, 539 (D. Md. 2011) (stating that "it is highly unlikely – indeed almost unimaginable – that a cell phone would remain within public spaces"); State v. Earls, 70 A.3d 630, 652 (N.J. Sup. Ct. 2013) ("Law enforcement had no way of knowing in advance whether defendant's cell phone was being monitored in a . . . private space."); *Kyllo*, 533 U.S. at 38-39. Under the *Kyllo* standard, any searches of private residences conducted by technology not available to the general public that could not otherwise have been conducted without a warrant are unconstitutional. *See id.* The use of cell site simulators is patently exclusive to government law enforcement and should violate the *Kyllo* standard every time they are used to track cell phone location information in real-time. *See id.*