ARTICLES

THE FOURTH AMENDMENT IMPLICATIONS OF THE GOVERNMENT'S USE OF CELL TOWER DUMPS IN ITS ELECTRONIC SURVEILLANCE

The Honorable Brian L. Owsley[*]

Privacy concerns resonate with the American people. Although the right to privacy is not explicitly protected in the United States Constitution, the Supreme Court has found the right to privacy rooted within the Constitution based on various amendments.[1] In the modern era, with rapid advances in technology, threats to privacy abound, including new surveillance methods by law enforcement. There is a growing tension between an individual's right to privacy and our collective right to public safety. This latter right is often protected by law enforcement's use of electronic surveillance as an investigative tool, but such surveillance may at times be done in a way that is inconsistent with constitutional rights.

Recently, the American Civil Liberties Union brought to light the popular use of government surveillance of cell phones, including the gathering of all cell phone numbers utilizing a specific cell site location.[2] Known as a "cell tower dump," such procedures essentially ob-

---

* Brian L. Owsley, Visiting Assistant Professor, Texas Tech University School of Law; B.A., 1988, University of Notre Dame, J.D., 1993, Columbia Law School, M.I.A., 1994, Columbia University School of International and Public Affairs. From 2005 until 2013, the author served as a United States Magistrate Judge for the United States District Court for the Southern District of Texas. This Article was written in the author's private capacity. No official support or endorsement by the United States District Court for the Southern District of Texas or any other division of the federal judiciary is intended or should be inferred. I am very grateful for valuable comments and critiques provided by Susan Freiwald, Jonah Horwitz, Orin Kerr, Stephanie Pell, Stephen Wm. Smith, and Christopher Soghoian.

1 *See* Katz v. United States, 389 U.S. 347, 350–51 (1967) (discussing the emanation of the constitutional right to privacy from the Fourth Amendment); Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (discussing the emanation of the constitutional right to privacy from the First, Third, Fourth, Fifth and Ninth Amendments).

2 Press Release, American Civil Liberties Union, ACLU Releases Cell Phone Tracking Documents From Some 200 Police Departments Nationwide (Apr. 2, 2012), *available at* http://www.aclu.org/national-security/aclu-releases-cell-phone-tracking-documents-some-200-police-departments-nationwide; American Civil Liberties Union, ACLU Affiliate

tain all of the telephone number records from a particular cell site tower for a given time period: "A tower dump allows police to request the phone numbers of all phones that connected to a specific tower within a given period of time."[3] State and federal courts have barely addressed cell tower dumps.[4] However, the actions by most of the largest cell phone providers, as well as personal experience and conversations with other magistrate judges, strongly suggest "that it has become a relatively routine investigative technique" for law enforcement officials.[5]

No federal statute directly addresses whether and how law enforcement officers may seek a cell tower dump from cellular telephone providers. Assistant United States Attorneys, with the encouragement of the United States Department of Justice, apply for court orders authorizing cell tower dumps pursuant to a provision in the Electronic Communications Privacy Act of 1986.[6] The pertinent provision poses a procedural hurdle less stringent than a warrant based on probable cause, which in turn raises significant constitutional concerns.

This Article provides a brief description of cellular telephone and cell-site technology in Part I. Next, Part II addresses the evolution of Fourth Amendment jurisprudence and argues that the reasonable expectation of privacy standard applies to electronic surveillance such

---

Nationwide Cell Phone Tracking Public Record Requests Findings and Analysis (Mar. 31, 2012), *available at* http://www.aclu.org/files/assets/cell_phone_tracking_documents_-_final.pdf.

3 Jeffrey Brown, *What Type of Process is Required for a Cell Tower Dump?*, CYBERCRIME REV. (May 16, 2012), http://www.cybercrimereview.com/2012/05/what-type-of-process-is-required-for.html.

4 There are only a few decisions discussing this surveillance technique in the United States. *See* United States v. Duffey, No. 3:08-CR-0167-B, 2009 WL 2356156, at *1 (N.D. Tex. July 30, 2009); Jackson v. State, 716 S.E.2d 188, 190 (Ga. 2011). In Canada, there is also a reported case addressing cellular telephone records obtained through a cell tower dump. *See generally* R. v. Mahmood (2008), 2008 CanLII 51774 (ON SC), 2008 O.J. No. 3922, 236 C.C.C. 3d 3, 79 W.C.B. 2d 366 (Can. Ont. Sup. Ct. J. 2008), *aff'd* 2011 CanLII 693 (Can. Ont. C.A. 2011). Since the inception of this Article, I have issued two decisions denying requests for cell tower dumps and one decision granting a request for a cell tower dump. *See In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(D), No. C-13-497M, 2013 WL 1934491 (S.D. Tex. May 8, 2013) (denying); *In re* Search of Cellular Telephone Towers, Nos. C-13-523M, C-13-525M, C-13-526M, C-13-527M, C-13-528M, 2013 WL 1932881 (S.D. Tex. May 8, 2013) (granting); *In re* United States *ex rel.* Order Pursuant to 18 U.S.C. § 2703(D), Nos. C-12-670M, C-12-671M, C-12-672M, C-12-673M, 2012 WL 4717778 (S.D. Tex. Sept. 26, 2012) (denying).

5 Timothy B. Lee, *Documents Show Cops Making up the Rules on Mobile Surveillance*, ARS TECHNICA (Apr. 3, 2012, 10:40 AM.), http://arstechnica.com/tech-policy/2012/04/documents-show-cops-making-up-the-rules-on-mobile-surveillance/.

6 Pub. L. No. 99-509, 100 Stat. 1848 (1986).

as cell tower dumps. In Part III, the discussion follows the development of statutes addressing electronic surveillance and posits that cell tower dumps request more information than simply telephone numbers. Part IV analyzes records from both cellular service providers and the federal government to conclude that cell tower dumps routinely occur. Part V assesses the few decisions that discuss cell tower dumps and argues that the constitutional analysis is either nonexistent or flawed regarding the use of the Stored Communications Act to permit cell tower dumps. Next, Part VI asserts that cell tower dumps cannot be analyzed pursuant to the Stored Communications Act because the language of the statute is inapplicable and the amount of information sought requires a warrant based on probable cause. This Part concludes by proposing some protocols to safeguard individual privacy rights.

I. CELL SITE TOWERS GATHER INFORMATION ABOUT ALL CELLULAR TELEPHONES OPERATING WITHIN THEIR RADII

In 1986, Congress enacted the Electronic Communications Privacy Act, which in part concerned the then new technology of cellular telephones that were based on radio transmission.[7] In order for these telephones to function, cellular telephone providers operate "large service areas [that] are divided into honeycomb-shaped segments or 'cells'—each of which is equipped with a low-power transmitter or base station which can receive and radiate messages within its parameters."[8] One commenter has described cell site data as

> a collection of a number of pieces of data "regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites, as

7 *See In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority (*Southern Texas Order 1*), 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005) ("A cell phone is a sophisticated two-way radio with a low-power transmitter that operates in a network of cell sites."); *In re* Application of U.S. for Historical Cell Site Data (*Southern Texas Order 2*), 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010) ("[C]ellular telephones use radio waves to communicate between the user's handset and the telephone network.").

8 S. Rep. No. 99-541, at 9 (1986); *see also Southern Texas Order 1*, 396 F. Supp. 2d at 750 ("'Cell' refers to geographic regions often illustrated as hexagons, resembling a bee's honeycomb; a 'cell site' is where the radio transceiver and base station controller are located (at the point three hexagons meet."); Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 126 (2012) ("Service providers maintain large numbers of radio base stations (also called 'cell sites') spread throughout their geographic coverage areas. These cell sites are generally located on 'cell towers' serving geographic areas of varying sizes, depending upon topography and population concentration.").

> well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture."[9]

At each cell (or cell site), there is a wireless antenna that "detects the radio signal from the handset, and connects it to the local telephone network, the Internet, or another wireless network."[10] Although many cell sites are physically located on towers, they can also be placed on trees, roofs, flagpoles, the sides of buildings, or even inside buildings.[11] Smaller cell site units known as microcells, picocells, or femtocells are typically used in buildings operating with much smaller service areas to boost coverage and decrease dead zones.[12]

Whenever someone uses a cellular telephone, it triggers a series of relays along the cell-site network:

> When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone . . . moves from cell to cell.[13]

The number of cell sites in a geographical area depends in part on the density of cell phone users. Thus, typically in rural areas, there

---

9 Ian Herbert, *Where We Are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, 16 BERKELEY J. CRIM. L. 442, 478 (2011) (quoting *Southern Texas Order 1*, 396 F. Supp. 2d at 749).

10 *Southern Texas Order 2*, 747 F. Supp. 2d at 831.

11 *Id.* ("No longer just big three-sided radio towers, base station antennas can be mounted outdoors on roof-tops, building-sides, trees, flagpoles, and church steeples, or indoors in homes and offices.").

12 *See, e.g.*, N.Y. SMSA Ltd. P'ship v. Town of Clarkstown, 612 F.3d 97, 101–02 (2d Cir. 2010) (per curiam) (addressing microcells and distributed antenna systems); Omnipoint Holdings, Inc. v. City of Cranston, 586 F.3d 38, 44 (1st Cir. 2009) (discussing a potential use of microcells); *Southern Texas Order 2*, 747 F. Supp. 2d at 833 (explaining the accuracy and precision of the new technologies); *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 25 (2010) (statement of Professor Matt Blaze), *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf (stating that the increase of cellular base towers has "accelerated with the deployment of the latest generation of smaller and smaller-scale base stations . . . designed to serve very small areas "); Lachlan Paige, *Mapping Human Behavior: How Cell Tower Data, Social Media Geolocation and Pattern Analysis Help Investigators*, 38 LAW ENFORCEMENT TECH. 24, 29 (2011) ("'Picocells'—smaller sites that have 360-degree coverage and are mounted on telephone poles rather than taking up land—are a cost-effective solution for carriers that want to boost signal without building or leasing new towers.").

13 S. Rep. No. 99-541, at 9 (1986); *see also* Pell & Soghoian, *supra* note 8, at 127 ("[M]obile telephones (as their name suggests) are portable, and so when a phone moves away from the cell site with which it started a call and nearer to a different cell site, the call is 'handed over' from one cell site to another without interruption.").

will be fewer cell sites, while in large cities there will be many more cell sites. Any time a person's cell phone is turned on, that telephone is sending out a signal testing what is the nearest cell site, which in turn registers with that cell site.[14] "This process, called 'registration', [sic] occurs approximately every seven seconds."[15] Registration enables cellular providers to obtain a plethora of information about the telephones contacting their cell sites.

Cellular telephone providers have to be able to gather and store information through registration regarding cell phones that interact with their cell towers. "In order to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular cell phone, the portion of that tower facing the phone, and often the signal strength of the phone."[16] These providers "generally keep detailed historical records of this information for billing and other business purposes."[17] Indeed, depending on various factors, this information can be used to determine a phone's location to within a few hundred yards.[18]

---

14 *ECPA Reform and the Revolution in Location Based Technologies and Services*, *supra* note 12 at 13–14.

15 *In re* Application of U.S. for an Order Directing a Provider of Electronic Commc'n Serv. to Disclose Records to the Gov't (*Western Pennsylvania Order*), 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008) (footnote omitted), *rev'd and vacated on other grounds* (*Third Circuit Order*), 620 F.3d 304, 313 (3d Cir. 2010).

16 U.S. DEPT. OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL, at 41 (rev. 2005) [hereinafter ELECTRONIC SURVEILLANCE MANUAL], *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf; *see also In re* Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information (*Eastern New York Order 1*), 809 F. Supp. 2d 113, 115 (E.D.N.Y 2011) ("Cell phones work by communicating with cell-sites operated by cell-phone service providers. Each cell-site operates at a certain location and covers a certain range of distance."). Indeed, the Federal Communications Commission has issued regulations that "require cellular service providers to upgrade their systems to identify more precisely the longitude and latitude of mobile units making emergency 911 calls." *In re* Application of U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone (*Maryland Order 1*), 849 F. Supp. 2d 526, 532 (D. Md. Aug. 3, 2011); *see also* 47 C.F.R. § 20.18(h) (setting accuracy standards for cell phone calls within targeted distances).

17 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 16, at 41; *see also In re* Application of U.S. for and [sic] Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services (*Western Texas Order*), 727 F. Supp. 2d 571, 573 (W.D. Tex. 2010) ("[Cell site location information] is information that resides on computer servers of telecommunications providers."); Pell & Soghoian, *supra* note 8, at 128 ("Wireless service providers retain detailed logs for diagnostic, billing, and other purposes.").

18 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 16, at 41; *see also Eastern New York Order 1*, 809 F. Supp. 2d at 115 (explaining that several factors, including population density, determine the distance between cell sites); Pell & Soghoian, *supra* note 8, at 176 ("[T]he precision of the location information these technologies produce has increased dramati-

A law enforcement official requesting a cell tower dump seeks to collect all of the historical records that providers maintain from a specific cell tower or towers. These "records provide a listing of any cell phones that have utilized the cell phone tower for a particular time and date."[19] As with all historical cell site data, these records do not establish an exact location, but instead give a general location of the cell phone.[20] As one wireless technology expert explained, cell tower dumps "can be especially useful with serial crimes such as home invasions, robberies or sexual assaults, because tower dumps for each crime location can be cross-referenced for numbers that come up in all locations."[21] Significantly, with the increased usage of picocells and femtocells, historical cell-site information can be as accurate as GPS, and in some cases even more accurate.[22]

II. FOURTH AMENDMENT JURISPRUDENCE HAS EVOLVED TO PROTECT SEARCHES BASED ON ELECTRONIC SURVEILLANCE

The Founders enshrined within the Fourth Amendment "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[23] It further provides that "no Warrants shall issue, but upon probable cause."[24] When the privacy implicated by the Fourth Amendment is involved and law enforcement agents are conducting a "search and seizure," the Supreme Court has indicated that a warrant is generally necessary.[25]

---

cally, such that a single cell tower data—particularly where enhanced by some of the 350,000 femtocells deployed around the country—is becoming as accurate as GPS.") (citing *In re* 2010 S.D. Tex. Application, 747 F. Supp. 2d 827, 834 (S.D. Tex. 2010); Press Release, Informa Telecoms & Media, The Shape of Mobile Networks Starts to Change as Femtocells Outnumber Macrocells in U.S. (Oct. 21, 2010), *available at* http://femtoforum.org/fema/pressreleases.php?id=269).

19 Criminal Complaint at 13, United States v. Capito (D. Ariz. Mar. 12, 2010) (No. 3:10-CR-8050).

20 *Id.*

21 Christa Miller, *Why and How to Add Mapping to Your Cell Phone Evidence*, COMM. TECH. SERV. (July 19, 2011), http://cops2point0.com/2011/07/why-how-add-mapping-your-cell-phone-evidence/comment-page-1/ (internal quotation marks omitted).

22 Christopher Soghoian, *Technologies of Tracking: An Introduction*, Yale Information Society Project, Location Tracking and Biometrics Conference (Mar. 3, 2013), http://www.youtube.com/watch?v=OwutGSjNQ0k.

23 U.S. CONST. amend. IV.

24 *Id.*; *see also* FED. R. CRIM. P. 41 (addressing the issuance of warrants, including for the seizure of electronically stored information).

25 *See, e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971) ("[T]he most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth

Of course, when the Fourth Amendment was originally contemplated, electronic surveillance was not an issue. Over time, the Fourth Amendment has been construed to extend protection from warrantless searches in numerous contexts as technological devices have developed. This development informs our view of the constitutional implications of cell tower dumps.

Originally, Fourth Amendment protections covered physically invasive searches, particularly of homes, but were eventually extended to cover intangibles.[26] Upon being jailed, the petitioner in *Ex parte Jackson* filed a writ of habeas corpus challenging his conviction for using the postal system to send a circular advertising a lottery that offered prizes in violation of federal law.[27] The Supreme Court addressed a Fourth Amendment challenge to the search and seizure of mail in the postal service's custody.[28] The *Jackson* Court explained, in dicta, that mail that had been sealed was subject to protection from unreasonable search and seizure:

> Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands of

---

Amendment—subject only to a few specifically established and well-delineated exceptions.'" (quoting Katz v. United States, 389 U.S. 347, 357 (1967)); *see also* William W. Greenhalgh & Mark J. Yost, *In Defense of the "Per Se" Rule: Justice Stewart's Struggle to Preserve the Fourth Amendment's Warrant Clause*, 31 AM. CRIM. L. REV. 1013, 1041 (1994) ("A long line of cases from 1789-1958 recognized that for a search to be valid under the Fourth Amendment, that search must either be pursuant to a valid warrant or fall within one of the recognized exceptions to the warrant requirement."). *But see* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994) (espousing the position that searches do not require a warrant per se but instead must be reasonable); Edwin J. Butterfoss, *Bright Line Breaking Point: Embracing Justice Scalia's Call for the Supreme Court to Abandon an Unreasonable Approach to Fourth Amendment Search and Seizure Law*, 82 TUL. L. REV. 77, 94–95 (2007) (describing how the Court has been unwilling to adopt a per se warrant approach with a strong warrant requirement).

26 *See* Boyd v. United States, 116 U.S. 616, 625–28 (1886) (holding that it does not require actual entry upon premises and search for and seizure of papers to constitute an unreasonable search and seizure within the meaning of the Fourth Amendment); *see also* Georgia v. Randolph, 547 U.S. 103, 143 (2006) (Scalia, J., dissenting) ("From the date of its ratification until well into the 20th century, violation of the [Fourth] Amendment was tied to common-law trespass." (citing Kyllo v. United States, 533 U.S. 27, 31–32 (2001)).

27 *Ex parte* Jackson, 96 U.S. 727 (1878).

28 *Id.* at 728 (citing Rev. St. § 3894).

> officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.[29]

The Court ultimately denied the petition challenging a law that barred using the federal mail to send lottery circulars.[30] Significantly, however, this dictum extended Fourth Amendment jurisprudence to private communications.

The evolution of Fourth Amendment jurisprudence continued with *Boyd v. United States*. The Supreme Court considered whether the "compulsory production of a man's private papers, to be used in evidence against him in a proceeding to forfeit his property for alleged fraud against the revenue laws . . . [constitutes] an '*unreasonable* search and seizure' within the meaning of the Fourth Amendment . . . ."[31] Ultimately, the Court held that the order to produce the invoice as well as the law authorizing its production were unconstitutional, so the judgment was reversed and remanded for a new trial.[32] The decisions in *Boyd* and *Jackson* laid the framework for the property-centric theory that guided Fourth Amendment jurisprudence well into the twentieth century.

When the Supreme Court first dealt with a challenge to the use of telephone wiretaps, it held that there was no Fourth Amendment violation.[33] In *Olmstead*, the government was investigating a conspiracy to possess and sell alcohol during Prohibition.[34] During this investigation, "[s]mall wires were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants."[35] Chief Justice William Howard Taft explained that persons subscribing to telephone service intend to project their voices outside their residences:

> Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment. The

---

29 *Id.* at 733; *see also* Wesley MacNeil Oliver, *America's First Wiretapping Controversy in Context and as Context*, 34 HAMLINE L. REV. 205, 210–15 (2011) (discussing the historical context of this dicta).

30 *Jackson*, 96 U.S. at 736–37.

31 *Boyd*, 116 U.S. at 622 (emphasis in original).

32 *Id.* at 638.

33 Olmstead v. United States, 277 U.S. 438 (1928).

34 *Id.* at 455–56.

35 *Id.* at 456–57.

> reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation.[36]

Instead, Fourth Amendment jurisprudence required a more narrow interpretation so that a violation occurred only when "there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house . . . ."[37] Consequently, the Court held "that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment."[38]

In dissent, Justice Louis Brandeis predicted that "'in the application of a constitution, our contemplation cannot be only of what has been but of what may be.' The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping."[39] Of course, as technology developed, Justice Brandeis' cautionary words proved to be quite accurate.

Furthering the reasoning of *Olmstead*, in *Goldman v. United States*, the Supreme Court heard a challenge to a conviction for essentially conspiracy to commit fraud in violation of the Bankruptcy Act.[40] After federal agents learned of an attempt by some lawyers to perpetrate a fraud on the bankruptcy court, they began an investigation into the fraud. Two agents, with the building manager's assistance but without a warrant, obtained access to the defendant's office at night and "installed a listening apparatus in a small aperture in the partition wall, with a wire to be attached to earphones extending into the adjoining office."[41] However, when "[t]hey connected the earphones to the apparatus . . . it would not work."[42]

Not to be deterred, the agents set up surveillance using a detectaphone placed against the wall of one of the attorney's offices to listen to and record, with the assistance of a stenographer, conversations

---

36 *Id.* at 465–66.

37 *Id.* at 466. This approach toward "Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century." United States v. Jones, 132 S. Ct. 945, 949 (2012) (citing Kyllo v. United States, 533 U.S. 27, 31 (2001)).

38 *Id.* at 466.

39 *Id.* at 474 (Brandeis, J., dissenting); *but see* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 Sup. Ct. Rev. 67, 69 (2012).

40 316 U.S. 129 (1942).

41 *Id.* at 131.

42 *Id.*

regarding the conspiracy.[43] Thus, instead of physically entering into the defendant's office, this device was operated from another office which the agents did not need a warrant to access. Analyzing the surveillance, the Court explained that

> [t]he listening in the next room to the words of [one attorney-conspirator] as he talked into the telephone receiver was no more the interception of a wire communication, within the meaning of the Act, than would have been the overhearing of the conversation by one sitting in the same room.[44]

Indeed, unlike the use of any information that would have been obtained by the original apparatus that failed, there was no trespass with the use of the detectaphone. [45] Because there was no invasion of the office, there was no Fourth Amendment violation.

Almost forty years after *Olmstead*, the Supreme Court, in *Katz v. United States*, addressed whether surveillance of a public telephone booth violated the Fourth Amendment. FBI agents were investigating the defendant for using a wire communication to engage in illegal gambling activity.[46] These agents did not wiretap the telephone booth where the defendant made his phone calls, but instead "attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls."[47] At trial, the prosecutor played these recordings over the defendant's objection.[48]

The *Katz* Court determined that *Olmstead* was no longer controlling because its reasoning had been eroded by subsequent decisions.[49] Justice Potter Stewart explained that a person who enters a telephone booth, "occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[50]

---

43 *Id.* at 130–31.

44 *Id.* at 134.

45 *Id.* at 134–35.

46 389 U.S. 347, 348 (1967).

47 *Id.* Although *Katz* was not a wiretap case, the Supreme Court had just enunciated the standards for a constitutional wiretap statute earlier in the Term. Berger v. United States, 388 U.S. 41, 64 (1967) (striking down New York's wiretap law).

48 *Katz*, 389 U.S. at 348.

49 *Id.* at 353; *see also Eastern New York Order 1*, 809 F. Supp. 2d 113, 126 (E.D.N.Y. 2011) (noting that the *Katz* decision "drastically changed existing Fourth Amendment doctrine"). Nonetheless, the Supreme Court has explained that while Katz amplified the "reasonable expectation of privacy" approach to Fourth Amendment jurisprudence, it did not repudiate the historical trespass approach. United States v. Jones, 132 S. Ct. 945, 950 (2012).

50 *Katz*, 389 U.S. at 352. *But see* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 821 (2004) ("Exactly

He continued by noting that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[51] Consequently, the Court concluded that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[52]

More than forty years later, in *City of Ontario v. Quon*, a rare decision by the Supreme Court concerning the Stored Communications Act, Justice Anthony Kennedy addressed the Court's reversal of *Olmstead* in *Katz*, explaining that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[53] This cautious approach contrasts with the Supreme Court's acknowledgment that its decisions regarding electronic surveillance must also consider new developments in that surveillance. For example, when the Court found the use of heat-sensing technology to be a search in *Kyllo v. United States*, it announced that "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[54] These two divergent approaches addressed in *Quon* and *Kyllo* demonstrate the tension and difficulty the Supreme Court and, consequently, the lower courts face regarding the collection of telephone numbers and other information through cell tower dumps.

People tend to expect that their locations, including those disclosed by historical cell-site data, are not readily accessible to law enforcement. The Supreme Court has explained that "[a] 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[55] The Supreme Court has concluded that this reasonable expectation extends to various areas that

---

why the user of the phone booth was constitutionally entitled to his privacy was left to the reader's imagination.").

51 *Katz*, 389 U.S. at 352.

52 *Id.* at 353.

53 130 S. Ct. 2619, 2629 (2010) (discussing the transition from the trespass approach in *Olmstead* to the deviation from the property-based approach in *Katz*); *accord In re* Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information (*Eastern New York Order 2*), 736 F. Supp. 2d 578, 595 (E.D.N.Y. 2010) (citation omitted); *see also* Clifford S. Fishman, *Electronic Privacy in the Government Workplace and* City of Ontario, California v. Quon: *The Supreme Court Brought Forth a Mouse*, 81 MISS. L.J. 1359, 1384–1405 (2012) (analyzing *City of Ontario v. Quon*).

54 533 U.S. 27, 36 (2001).

55 United States v. Jacobsen, 466 U.S. 109, 113 (1984) (citations omitted).

affect most people's daily lives: a home;[56] a vehicle;[57] a business premise;[58] a hotel room;[59] a storage locker;[60] a telephone booth;[61] and mail.[62] With the exception of telephone booths, which practically no longer exist, and postal mail, which may not exist in the near future, these examples are all places in which people routinely take and use their cell phones.[63]

This development of Fourth Amendment jurisprudence, particularly the notion of a reasonable expectation of privacy, influences how people view privacy, including their cell-site location data. In a poll that "attempted to assess whether Californians would support strong judicial intervention before law enforcement accessed historical location data," people were asked "Would you favor a law that required the police to convince a judge that a crime has been committed before obtaining location information from the cell phone company?"[64] In response, 73% of people supported or strongly sup-

---

56 *Kyllo*, 533 U.S. at 31 ("With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.") (citations omitted)); 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.") (citations omitted)).

57 United States v. Jones, 132 S. Ct. 945, 949 (2012) ("[T]he Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" (footnote omitted)); United States v. Chadwick, 433 U.S. 1, 12 (1977) ("[A]utomobiles are 'effects' under the Fourth Amendment, and searches and seizures of automobiles are therefore subject to the constitutional standard of reasonableness.").

58 *See, e.g.*, Marshall v. Barlow's, Inc., 436 U.S. 307, 311 (1978) ("The Warrant Clause of the Fourth Amendment protects commercial buildings as well as private homes."); See v. City of Seattle, 387 U.S. 541, 543 (1967) ("The businessman, like the occupant of a residence, has a constitutional right to go about his business free from unreasonable official entries upon his private commercial property.").

59 *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 301 (1966) ("A hotel room can clearly be the object of Fourth Amendment protection as much as a home or an office." (citation omitted)); Stoner v. California, 376 U.S. 483, 487–88 (1964) (rejecting the argument that a search of a hotel room, although conducted without the petitioner's consent, was lawful because it was conducted with the consent of the hotel clerk).

60 United States v. Karo, 468 U.S. 705, 720 n.6 (1984).

61 Katz v. United States, 389 U.S. 347, 352 (1967) ("[A] person in a telephone booth may rely upon the protection of the Fourth Amendment.").

62 United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable." (citations omitted)).

63 One scholar has posited that "[a]lthough the phrase 'reasonable expectation of privacy' sounds mystical, in most (though not all) cases, an expectation of privacy becomes 'reasonable' only when it is backed by a right to exclude borrowed from real property law." Kerr, *supra* note 50, at 809–10.

64 Jennifer King & Chris Jay Hoofnagle, *Research Report: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Location Information*, FED. TRADE COMM'N 8

ported this requirement.[65] Indeed, numerous groups and entities across the political spectrum view warrants as a prerequisite to obtaining location data:

> Not only civil liberties groups insist that warrants to track the whereabouts of Americans—or at least their cell phones—are necessary. A coalition that formed in March includes Google, Microsoft, AOL, eBay, Intel, Qwest, AT&T, and conservative and libertarian groups including Americans for Tax Reform and the Progress and Freedom Foundation.[66]

Ultimately, most survey participants expect their cell-site location information to be private. This expectation coupled with the development of Fourth Amendment jurisprudence—most notably *Katz*—supports the position that Fourth Amendment protections extend to cell tower dumps.

III. THE DEVELOPMENT OF FOURTH AMENDMENT JURISPRUDENCE ALONG WITH DEVELOPMENTS IN TECHNOLOGY LED CONGRESS TO ENACT LEGISLATION TO PROTECT INDIVIDUALS' PRIVACY FROM ELECTRONIC SURVEILLANCE

In 1968, in response to the Supreme Court's decisions in *Katz* and *Berger v. New York*,[67] Congress enacted the Omnibus Crime Control and Safe Streets Act, which amended the law authorizing wiretaps.[68] In 1986, Congress enacted the Electronic Communications Privacy Act, which included the Stored Communications Act.[69] The Electronic Communications Privacy Act[70] was designed to "protect against the unauthorized interception of electronic communications."[71] Fur-

---

(Apr. 18, 2008), *available at* http://www.ftc.gov/os/comments/mobilevoice/534331-00005.pdf.

65 *Id.* at 8–9; *see* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 744 (2011) (describing how most users view their location data as private information and expect it to remain private).

66 Declan McCullagh, *ACLU: FBI Used 'Dragnet'-Style Warrantless Cell Tracking*, CNET NEWS (June 22, 2010, 9:37 AM PDT), http://news.cnet.com/8301-31921_3-20008444-281.html (citation omitted).

67 388 U.S. 41, 54–60 (outlining the steps necessary for a wiretap statute to be constitutional).

68 Pub. L. No. 90-351, 82 Stat. 197 (1968). Congress first enacted a statute authorizing wiretaps in 1934. 48 Stat. 1064 (1934).

69 Stored Wire and Electronic Communications and Transactional Records Access, Pub. L. No. 99-508, § 201, 100 Stat. 1861 (Oct. 21, 1986) (codified as amended at 18 U.S.C. §§ 2701–2710); *see also* Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 607–09 (2007) (discussing the Stored Communications Act).

70 Pub. L. No. 99-508, 100 Stat. 1848 (1986).

71 S. Rep. No. 99-541, at 1 (1986); *Maryland Order 1*, 849 F. Supp. 2d 526, 571; *see also* Bankston, *supra* note 69, at 607 (describing how the new act protected electronic communica-

thermore, Congress sought to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[72] Courts have noted that the purpose of the Stored Communication Act is to protect and balance people's privacy with the government's law enforcement activities.[73]

Despite the statute's purported attempt to preserve privacy rights, the Stored Communications Act allows the government to obtain electronic communications records from providers based on standards less demanding than probable cause:

> 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 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 by a court with jurisdiction over the offense under investigation or equivalent State warrant;
>
> (B) obtains a court order for such disclosure under subsection (d) of this section;
>
> (C) has the consent of the subscriber or customer to such disclosure;
>
> (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing . . . ; or
>
> (E) seeks information under paragraph (2).[74]

---

tions as well as wire and oral communications); Robert A. Pikowsky, *The Need For Revisions To The Law Of Wiretapping And Interception Of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 39 (2003) (explaining how the Electronic Communications Privacy Act amended the federal Wiretap Act in order to protect the privacy of electronic communications).

72 S. Rep. No. 99-541, at 1; *Maryland Order 1*, 849 F. Supp. 2d, at 571; Pikowsky, *supra* note 71, at 39 ("The[se] statutory amendments established a privacy interest for parties to cellular telephone conversations . . . .").

73 United States v. Warshak, 631 F.3d 266, 335 (6th Cir. 2010) (Keith, J., concurring) ("The purpose of § 2703, along with the Stored Communications Act as a whole, is to maintain the boundaries between a citizen's reasonable expectation of privacy and crime prevention in light of quickly advancing technology." (citing S. Rep. 99-541, at 4)); Theofel v. Farey-Jones, 359 F.3d 1066, 1072 (9th Cir. 2004) ("[T]he Stored Communications Act protects individuals' privacy and proprietary interests. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage as a communications facility."); Penrose Computer Marketgroup, Inc. v. Camin, 682 F. Supp. 2d 202, 209 (N.D.N.Y. 2010) ("The purpose of the SCA was, in part to protect privacy interests in personal and proprietary information and to address 'the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public.'") (citations omitted)).

74 18 U.S.C. § 2703(c)(1) (2006).

Subscriber or customer information also available based on a law enforcement request may include the person's name; address; telephone call records, including times and durations; lengths and types of services; subscriber number or identity; means and source of payment, including bank account number or credit card number; date of birth; social security number; and driver's license number.[75] Indeed, any of this information is available simply by presenting the telecommunications provider with a subpoena.[76]

To obtain records other than those just specified, including cell-site location data, the government must obtain *either* a warrant *or* a court order. In obtaining a court order, a law enforcement officer must simply present the court with "*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.*"[77]

> Some scholars have referred to the D Order standard as a "Terry-stop" standard, a reference to *Terry v. Ohio*, where the Supreme Court created the reasonable suspicion standard for sidewalk stop-and-frisk encounters. The *Terry* standard is met when an officer "point[s] to specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch of criminal activity.[78]

As courts have noted, the "specific and articulable facts" standard creates a lesser burden than the requirement of a warrant based on probable cause. The Third Circuit has explained that "the [Act's] legislative history provides ample support for the proposition that the

---

75 18 U.S.C. § 2703(c)(2); *accord In re* § 2703(d) Order, 787 F. Supp. 2d 430, 436 (E.D. Va. 2011); *see also In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d) (*Southern New York Order 1*), 157 F. Supp. 2d 286, 288 (S.D.N.Y. 2001) (describing an order pursuant to § 2703 authorizing the government to receive "the subscriber's name, home address, telephone number, e-mail address and any other identifying information [the provider] may have, such as date of birth, social security number, driver's license number and billing information").

76 18 U.S.C. § 2703(c)(2); *see also* United States v. Orozco, 456 F. App'x 149, 151–52 (3d Cir. 2012) (records obtained by subpoena as opposed to a warrant were admissible); *Third Circuit Order*, 620 F.3d 304, 313–14 (3d Cir. 2010) (discussing the use of subpoena to obtain records pursuant to § 2703(c)(2)).

77 18 U.S.C. § 2703(d) (emphases added). Even the United States Department of Justice acknowledges that "[t]he requirements for obtaining a section 2703(d) court order must be met even if the government seeks the court order only to obtain subscriber and telephone information." ELECTRONIC SURVEILLANCE MANUAL, *supra* note 5, at 18.

78 Pell & Soghoian, *supra* note 8, at 151–52 (citations omitted); *see generally* Terry v. Ohio, 392 U.S. 1 (1968).

standard is an intermediate one that is less stringent than probable cause."[79]

In 1979, the Supreme Court established that a person has no reasonable expectation of privacy in the telephone numbers he or she dials.[80] In *Smith v. Maryland*, law enforcement agents used a pen register, which records the outgoing dialed telephone numbers on a specific telephone. "A 'pen register' is a device used, inter alia, to record the dialing and other information transmitted by a targeted phone."[81] The counterpart to a pen register is a trap-and-trace device, which records the incoming dialed telephone numbers on a specific telephone.[82] Nonetheless, the principles outlined in *Smith* concerning the expectation of privacy in telephone numbers apply equally to the analysis of applications pursuant to § 2703.

When law enforcement obtains just a suspect's cell phone number, because no search has been conducted, no Fourth Amendment right is implicated.[83] In *Smith*, the Supreme Court reasoned that

---

79 *Third Circuit Order*, 620 F.3d at 315; *see also* Peter P. Swire, Katz *is Dead. Long Live* Katz., 102 MICH. L. REV. 904, 910 (2004) (explaining how the Stored Communications Act allows law enforcement officers to obtain access to the stored communications from a communications provider without a warrant so that e-mail content may be accessed with a showing of less than probable cause).

80 Smith v. Maryland, 442 U.S. 735, 742 (1979) (rejecting the claims that people have a legitimate expectation of privacy regarding the numbers they dial on their phones); *see also* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("Therefore the use of a pen register is not a Fourth Amendment search. Importantly, the Court [in *Smith v. Maryland*] distinguished pen registers from more intrusive surveillance techniques on the ground that 'pen registers do not acquire the *contents* of communications' but rather obtain only the addressing information associated with phone calls." (emphasis in original)); United States v. Fregoso, 60 F.3d 1314, 1319 n.3 (8th Cir. 1995) ("'[I]nstallation and use of a pen register . . . [is] not a 'search' within the meaning of the Fourth Amendment and therefore its use does not violate the Constitution.'" (quoting *Smith*, 442 U.S. at 745–46); United States v. Thompson, 936 F.2d 1249, 1251 (11th Cir. 1991) (describing how *Smith v. Maryland* established that a device which merely records the numbers dialed from a particular telephone line does not represent a sufficient invasion of privacy to warrant Fourth Amendment protection); United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990) (same); Mack v. United States, 814 F.2d 120, 124 (2d Cir. 1987) (same).

81 United States v. Jadlowe, 628 F.3d 1, 6 n.4 (1st Cir. 2010); *accord In re* Application of U.S. for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (*Maryland Order 2*), 402 F. Supp. 2d 597, 602 (D. Md. 2005) ("[P]en register records telephone numbers dialed for outgoing calls from the target phone . . . .").

82 *Maryland Order 2*, 402 F. Supp. 2d at 602 ("[A] trap/trace device . . . records the telephone numbers of those calling the target phone"); *Southern Texas Order 1*, 396 F. Supp. 2d 747, 752 (S.D. Tex. 2005) ("A trap and trace device captures the numbers of calls made to the target phone.").

83 *See* Minnesota v. Dickerson, 508 U.S. 366, 375 (1993) (explaining that if "no invasion of a legitimate expectation of privacy" occurs, then "no 'search' within the meaning of the

"[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company," and they all understand "that the phone company has facilities for making permanent records of the numbers they dial."[84] Because the reasoning in *Smith* applies equally to cell phone users, they likewise have no reasonable expectation of privacy in their own phone numbers.[85]

However, unlike in *Smith*, in seeking a cell tower dump, the government routinely requests more information than just the telephone numbers dialed.[86] Often, the goal beyond developing a list of suspects in a criminal investigation is to track the location and movement of those suspects. Because the information sought pursuant to § 2703 exceeds just telephone numbers, *Smith* is inapplicable to the government's requests for a cell tower dump.

IV. RECORDS FROM BOTH LAW ENFORCEMENT OFFICERS AND TELECOMMUNICATIONS PROVIDERS INDICATE THAT CELL TOWER DUMPS ROUTINELY OCCUR

Cell tower dumps have not garnered much attention in the media. Indeed, the government does not like to draw attention to this elec-

---

Fourth Amendment" does either); *see also* United States v. Flores-Lopez, 670 F.3d 803, 807 (7th Cir. 2012) ("[B]y subscribing to the telephone service the user of the phone is deemed to surrender any privacy interest he may have had in his phone number." (citing *Smith*, 442 U.S. at 742–43)); United States v. Clenney, 631 F.3d 658, 666 (4th Cir. 2011) ("Phone customers have no constitutionally cognizable privacy interests in basic subscriber information.") (citing *Smith*, 442 U.S. at 743–46)); Rehberg v. Paulk, 611 F.3d 828, 843 (11th Cir. 2010) ("[A] person does not have a legitimate expectation of privacy in numerical information he conveys to a telephone company in the ordinary course of business." (citing *Smith*, 442 U.S. at 743–44)).

84 *Smith*, 442 U.S. at 742; *accord* United States v. Graham, 846 F. Supp. 2d 384, 401 (D. Md. 2012) (quoting *Smith*); United States v. Benford, No 2:09CR86, 2010 WL 1266507, at *2 (N.D. Ind. Mar. 26, 2010) (same); *see also In re* Application of U.S. for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device, 846 F. Supp. 1555, 1557 (M.D. Fla. 1994) (discussing *Smith* and rejecting any expectation of privacy where the phone numbers dialed by telephone users are transmitted through the telephone company, which also keeps records and provides bills with lists of telephone numbers dialed).

85 *See In re* Application of U.S. for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197, 199 (C.D. Cal. 1995) (citing *Smith*, 442 U.S. at 742–45).

86 *See* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 16, at 162 (demonstrating how extensive court orders for telephone electronic communication records can be); *see also Southern New York Order 1*, 157 F. Supp. 2d 268, 288 (S.D.N.Y. 2001) ("The Order requires Cablevision to provide the Government with the subscriber's name, home address, telephone number, e-mail address and any other identifying information Cablevision may have, such as date of birth, social security number, driver's license number and billing information.").

tronic surveillance method. Interestingly, in my own informal survey of magistrate judges nationwide, many have informed me that they were unfamiliar with cell tower dumps. After coming to an understanding of the procedure, numerous had concerns or reservations about them.

In August 2011, the American Civil Liberties Union sought records regarding electronic surveillance, including cell tower dumps, from numerous law enforcement agencies around the country.[87] Specifically, "35 ACLU affiliates filed over 380 public records requests with state and local law enforcement agencies to ask about their policies, procedures and practices for tracking cell phones."[88] Ultimately, it "received over 5,500 pages of documents from over 200 local law enforcement agencies regarding cell phone tracking."[89] The ACLU has made publicly available records it received from these requests.[90] It obtained these documents through public records requests from various law enforcement officials.[91]

Moreover, the production of cell-site location information has resulted in significant breaches of innocent third parties' privacy rights. In *United States v. Capito*, the government obtained records from cell towers near four separate bank robbery crime scenes in rural Arizona.[92] After obtaining responses to their requests from the various telecommunications providers, the FBI agents ultimately received over 150,000 telephone numbers.[93] In a Connecticut federal case, the cell tower dump revealed 180 different individuals' cell numbers, including the defendant who was ultimately convicted of bank robbery.[94]

---

87 *Cell Phone Location Tracking Public Records Request*, ACLU (Mar. 25, 2013), https://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request.

88 *Id.* In April 2012, an additional affiliate filed 27 requests. *Id.*

89 *Id.*

90 *Id.*

91 *Id.*

92 Criminal Complaint at 16, United States v. Capito (D. Ariz. Mar. 12, 2010) (No. 3:10-CR-8050).

93 *Id.* at 13. In a Canadian case, R. v. Mahmood, the warrants for the cell tower dumps covered only four cellular providers in a neighborhood in the greater Toronto metropolitan area. 2008 CanLII 51774 (ON SC), 2008 O.J. No. 3922, 236 C.C.C. 3d 3, 79 W.C.B. 2d 366, at ¶¶ 19, 96. Those requesting officers received records concerning 9,588 separate telephone calls by 7,067 different customers. Moreover, it revealed personal information regarding the telephone companies' subscribers, including the subscribers' names and addresses, information regarding their approximate geographic location on the date and at the time in question (that is, in the vicinity of the two cellular transmission towers), information regarding what telephone numbers they were calling and/or what numbers were calling them, and information regarding the duration of their calls. *Id.* at ¶ 19.

94 Memorandum in Support of Motion to Suppress at 7, United States v. Soto, (D. Conn. May 18, 2010) (No. 3:09-CR-200-AWT).

A. *Cellular Service Providers Routinely Provide Cell Tower Dump Records to Law Enforcement Officials*

The records obtained by the ACLU establish that various cellular telephone and Internet providers charge fees to provide law enforcement officers with information from a search of their subscribers' accounts.[95] For some providers, cell phone surveillance, including cell tower dumps, generates revenue.[96] For example, in 2011, Verizon "report[ed] that it had been 'reimbursed approximately three to five million dollars in each of the last five years' for the data" it provided to law enforcement.[97] Similarly, AT&T collected $8.3 million in fees, up from $2.8 million in 2007.[98] Although Sprint declined to provide any information about how much it collects in fees, commentators have estimated that it could be as high as $26 million, but probably at least $10 million.[99] Even U.S. Cellular, a small provider, reported earning $460,000 in fees from providing data in response to

---

95 *See* 18 U.S.C. § 2706 (2006) (addressing cost reimbursement); *see also* Mich. Bell Tel. Co. v. Drug Enforcement Admin., 693 F. Supp. 542, 544 (E.D. Mich. 1988) ("While not a model of legislative drafting, it is clear that Congress did not intend that service providers be compensated for costs of compliance for routine requests for toll or subscriber information. As a general rule, the government must pay service providers 'a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information' . . . ." (quoting 18 U.S.C. § 2706(a))). Moreover, those cell phone numbers are now available to anyone online. *See* McCullagh, *supra* note 66.

96 *See* Eric Lichtblau, *Police Are Using Phone Tracking as Routine Tool: Cell Companies Profit: Civil Libertarians Worry as Surveillance Skirts Court Oversight*, N.Y. TIMES, Apr. 1, 2012, at A1 ("The practice has become big business for cellphone companies, too, with a handful of carriers marketing a catalog of 'surveillance fees' to police departments to determine a suspect's location, trace phone calls and texts or provide other services."); Clarence Walker, *Warrantless Cell Phone Tapping? How Police May Be Secretly Tracking You*, ALTERNET (May 25, 2012), *available at* http://www.alternet.org/drugs/155604/warrantless_cell_phone_tapping_how_police_may_be_secretly_tracking_you ("Not only are the wireless providers profiting from your privacy by working with the police, they are lobbying to be able to continue to do so."); Lee, *supra* note 5 ("The documents also suggest that selling customer information to law enforcement has become a significant revenue source for cell phone companies."). *But see* Andy Greenberg, *These Are the Prices AT&T, Verizon and Sprint Charge for Cellphone Wiretaps*, FORBES (Apr. 3, 2012), *available at* http://www.forbes.com/sites/andygreenberg/2012/04/03/these-are-the-prices-att-verizon-and-sprint-charge-for-cellphone-wiretaps/ (quoting Verizon representing that it does not "make a profit from any of the data requests from law enforcement").

97 David Sydiongco & Will Oremus, *How Much Money Does Your Cellphone Company Make from Selling Your Data to Police?*, SLATE (July 19, 2012) (footnote omitted), http://www.slate.com/blogs/future_tense/2012/07/19/cellphone_spying_wireless_carriers_make_millions_tracking_customers_selling_data_to_police.html.

98 Eric Lichtblau, *Wireless Firms Are Flooded by Requests to Aid Surveillance*, N.Y. TIMES (July 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html.

99 *Id.*

law enforcement requests.[100] This interest in increasing revenue creates an incentive to cooperate with law enforcement that invariably leads to a loss of privacy by some innocent third parties.[101]

Each cellular telephone service provider has set fees for cell tower dumps. AT&T Mobility charges $50 per hour with a four-hour minimum for what it characterizes as "Tower Dumps."[102] It recommends "marking the service of the search warrant or court order URGENT" in order to receive an expedited response.[103] U.S. Cellular bills $50 for each staff hour for each cell tower dump when the requests require more than thirty minutes of staff time.[104] For what are described as "Cell Tower Searches," T-Mobile charges $100 per tower for each hour with the fee rounded up to the next hour for just a list of telephone numbers, but $150 per tower for each hour where the subscriber information is provided with each telephone number.[105] Verizon charges $30 per hour for "Cell site searches" conducted by the Legal Department systems and $60 per hour for each targeted tower if the search is done by the Network Department.[106] Verizon does not charge any additional fee for providing subscriber information related to the tower dump request.[107] Sprint/Nextel charges $50 a search for each tower and will also provide the subscriber with the telephone numbers if requested.[108] Indeed, records received by the ACLU provide an example in which the police department in Cary, North Carolina paid Sprint $500 for tower searches.[109] Typically, it provides this information in three to five days, but can provide it through expedited service for an additional charge.[110] Alltel Communication Wireless charges a flat fee of $500 for each tower search.[111]

---

100 *Id.*

101 Some carriers note that they lose money responding to these requests and that they are often not paid the fees on their submitted invoices. *See* Lichtblau, *supra* note 97.

102 Letter from Lisa A. Judge to Dan Pochoda at 87 (Sept. 6, 2011), ACLU, http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_tucsonpd_tucsonaz.pdf.

103 *Id.*

104 *Id.* at 123.

105 *Id.* at 88, 106.

106 *Id.* at 88, 115.

107 *Id.* at 88.

108 *Id.* at 89.

109 Letter from Michael Williams to Katherine Lewis Parker at 504 (Sept. 22, 2011), ACLU, *available at* http://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_carypd_carync. pdf.

110 Letter from Lisa A. Judge to Dan Pochoda, *supra* note 102, at 89.

111 *Id.* at 87.

According to an August 2010 chart prepared by the Computer Crime and Intellectual Property Section of the Department of Justice, each telecommunications provider has different retention periods regarding the cell towers used by phones.[112] Thus, Verizon keeps such information for about a year, Sprint/Nextel keeps it for at least eighteen months and up to two years, and AT&T has been keeping such records since July 2008.[113] Even though T-Mobile represents that it maintains cell tower records for no longer than six months, the Department of Justice indicated that such retention was likely more than a year.[114] In other words, these records are kept for long periods of time and the likelihood is that those periods of time will increase indefinitely such that the records will unlikely be destroyed. Most providers will probably follow AT&T's example of keeping the records indefinitely going forward.

One cell phone provider, Cricket Wireless,[115] does "not do cell site or tower dumps, nor do they call this type of request anything else."[116] Instead, it requires a phone number or name in order to provide information.[117] On the other end of the spectrum, AT&T Mobility even provided suggestions regarding specific language to use in any such request: "(electronic) Cell Tower Dump information for any and all cell phones that were used during (date and time frame) for the towers that cover this area (address information)."[118] It provides this guidance notwithstanding a company privacy policy representing that it does not sell its subscribers' information: "We will not sell your personal information to anyone, for any purpose. Period."[119] Of course, the records obtained by the ACLU flatly contradicted AT&T's assertion. In the end, AT&T sells its customers' information—

112 Retention Periods of Major Cellular Service Providers (U.S. Dep't of Justice), ACLU (Aug. 2010), http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart; David Kravets, *Which Telecoms Store Your Data the Longest? Secret Memo Tells All*, WIRED.COM (Sept. 28, 2011, 6:30 AM), http://www.wired.com/threatlevel/2011/09/cellular-customer-data/.

113 Retention Periods of Major Cellular Service Providers, *supra* note 112.

114 *Id.*

115 Unlike most cell phone providers with nationwide coverage, Cricket Wireless does not require a signed contract and utilizes prepaid plans. CRICKET WIRELESS, http://www.mycricket.com (last visited Aug. 9, 2013).

116 Letter from Lisa A. Judge to Dan Pochoda, *supra* note 102, at 89.

117 *Id.*

118 *Id.* at 87.

119 *Privacy Policy,* AT&T, http://www.att.com/gen/privacy-policy?pid=2506 (last visited Aug. 9, 2013). Other providers acknowledge using subscribers' personal information. For example, T-Mobile explains that it "use[s] personal information for a variety of business purposes." *Privacy Policy: Highlights*, T-Mobile, http://www.t-mobile.com/company/website/privacypolicy.aspx (last visited Aug. 8, 2013).

collecting $8.3 million in 2011—against its policy and more importantly, against the best interest of its customers. AT&T and other providers have capitalized on the sale of this customer information potentially at the expense of individual Fourth Amendment rights.

B. The Federal Government Routinely Utilizes Cell Tower Dump Records During Its Criminal Investigations

The wireless service providers' creation of master fee lists simply reflects law enforcement's growing interest in various types of surveillance as well as the providers' willingness to capitalize on such interest to generate additional income. Indeed, the United States Department of Justice has advised federal law enforcement officials that, generally, obtaining "[a] Court Order for a 'tower Dump' could provide valuable leads" in a criminal investigation.[120] It further explains that a cell tower dump is "[h]elpful when the location and time frame have been narrowed down, but *the target's phone number is unknown*."[121] However, this guide does not provide law enforcement officials with the basis for seeking a court order for this information or address the applicable legal standards. Moreover, it does not explain how the investigator is to discern the target phone number from all of the telephone numbers received.

Another Department of Justice internal publication, the *Electronic Surveillance Manual*, "sets forth the procedures established by the Criminal Division of the Department of Justice to obtain authorization to conduct electronic surveillance," including cell tower dumps.[122] The *Manual* provides the Department's attorneys with not only guidance, but form orders and form applications to use when seeking court orders and warrants to obtain electronic surveillance.

Regarding court orders pursuant to § 2703(d), the *Manual* specifically directs the Assistant United States Attorney to first

> appl[y] to the court for an order, pursuant to 18 U.S.C. § 2703(d), directing (provider of electronic communication service . . .) to disclose the (*choose as appropriate*: name; address; local and long distance telephone connection records, or records of session times and durations; length of service [including start date] and types of service utilized; telephone or instrument number or other subscriber number or identity, including

120 U.S. DEP'T OF JUSTICE, LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE 7 (rev. Mar. 10, 2010), *available at* http://cryptome.org/isp-spy/le-tel-spy.pdf.

121 *Id.* (emphasis added).

122 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 16, at ii.

> any temporarily assigned network address; means and source of payment for such service.[123]

Next, the attorney should certify "that it is believed that the subjects of the investigation are using the (*choose as appropriate:* telephone or instrument number; other subscriber number or identity . . .) in furtherance of the subject offenses; and that the information sought is relevant and material to an ongoing criminal investigation."[124] In other words, within such a certification, the Department of Justice acknowledges that some specific identifier, such as a telephone number or the subscriber's name, is necessary to obtain a court order pursuant to § 2703(d). This acknowledgment is significant because a cell tower dump requests large amounts of subscriber information without providing any specific identifier to obtain that information. In order to obtain records, including cell site location information, pursuant to § 2703, law enforcement officers must provide a specific phone number.[125]

V. THE FEW COURTS TO HAVE ADDRESSED CELL TOWER DUMPS HAVE IGNORED BOTH THE FOURTH AMENDMENT AND THE PRIVACY RIGHTS OF THOSE NOT TARGETED

The few existing judicial decisions addressing cell tower dumps establish that they can be a valuable weapon in law enforcement's arsenal. Moreover, the facts of these various cases demonstrate the types of criminal investigations in which officers have sought to utilize cell tower dumps. However, these decisions do not analyze the standard by which courts should authorize cell tower dumps. They also generally do not address Fourth Amendment concerns and seemingly never address the privacy issues related to individuals who are not the subject of the criminal investigation.

---

123 *Id.* at 162.

124 *Id.* (emphasis added). Similarly, another manual focusing on computer evidence, provides a proposed application for obtaining information pursuant to § 2703(d) utilizing a specific e-mail account. *See* U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 214 (2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

125 *See* In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), _ F. Supp. 2d _, 2013 WL 1934491, at *4 (S.D. Tex. May 8, 2013) (noting that the Assistant United States Attorney acknowledged that the application failed to provide any specific identifier as mandated by the Department of Justice's own guidance); *see also* In re U.S. For an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp. 2d 947, 952 (E.D. Wis. 2006) (stating that the Stored Communications Act provides records of specific subscribers or customers) (citing 18 U.S.C. § 2703(c)).

A. State Court in Georgia: Jackson v. State

In *Jackson v. State*, a jury convicted the appellant of several counts of burglary, false imprisonment, kidnapping, armed robbery, and aggravated assault as well as the murder of one of the victims.[126] The appellant and other accomplices had engaged in home invasions, where they robbed and assaulted their victims.[127] A third person had served as their driver, taking them to the robbery sites and then driving the getaway car.[128] During one robbery, the victims were being driven to their jewelry store when one of them noticed they were following another car that happened to be the getaway car.[129]

Regarding the cell tower dump, the court simply explained that "[d]uring the course of their investigation, police obtained cell phone numbers from a cell tower 'dump' from the tower nearest to the residences of the home invasions and the jewelry store."[130] The cell phone number for both the appellant and the getaway driver were among the numbers retrieved.[131]

On appeal, the appellant argued that the trial evidence was insufficient because it merely consisted of the getaway driver's uncorroborated testimony.[132] Regarding the evidence from the cell tower dump, he merely asserted "that the cell phone records are also not sufficient corroborating evidence as they only establish where his cell phone was at the time of the crimes, and not where he was, since he may have let a friend borrow his phone."[133] It does not appear that the appellant directly challenged the constitutionality of the cell tower dump itself. In affirming the conviction and sentence, the Supreme Court of Georgia concluded that the cell phone records, while cir-

126 716 S.E.2d 188, 189 (Ga. 2011).

127 *Id.* at 189–90.

128 *Id.*

129 *Id.* at 190.

130 *Id.*

131 *Id.* One commentator has noted that the *Jackson* case is the only state court decision mentioning tower dumps. Brown, *supra* note 3. Indeed, there is scant information available regarding the use of tower dumps by state law enforcement officials. However, in one recent case, two individuals were arrested for a series of burglaries throughout New England in which a cell tower dump was used to connect them to some of the crime scenes. *See* Karin Crompton, *Police Footwork Tracked Down Burglary Suspects*, THE DAY (Conn.) (updated Dec. 18, 2010, 1:49 PM), http://www.theday.com/article/20101218/NWS04/312189908.

132 *Jackson*, 716 S.E.2d at 190.

133 *Id.* at 191; *accord* Brown, *supra* note 3 (noting that "proper process was not an issue in that case").

cumstantial, were nonetheless sufficiently independent to constitute corroborating testimony.[134]

B. Federal Court in Texas: United States v. Duffey

In *United States v. Duffey*, the Northern District of Texas addressed a cell tower dump concerning an FBI investigation of "a group of armed robbers dubbed the 'Scarecrow Bandits' that [sic] had violently robbed more than twenty banks in the Dallas area."[135] During this investigation, the FBI utilized a cell tower dump to obtain cell phone records for the times and area around numerous bank robberies by the Scarecrow Bandits.[136] Specifically, these records established that the cell phones of two defendants were used near cell towers around the time of each of the robberies and that other Scarecrow Bandits' cell phones were linked to both these two defendants and cell towers near the banks.[137]

The cell phone records, as well as other information that the FBI obtained during its initial investigation, were used in turn to obtain wiretaps.[138] The defendants filed motions seeking to suppress the wiretaps.[139] Again, as in *Jackson*, in denying these motions, the court did not directly address any Fourth Amendment concerns about the cell tower dump. The federal prosecutors involved in the Scarecrow Bandits case maintain "that this was the first and the only time that the FBI has used the location-data-mining technique to nab bank

---

134 *Jackson*, 716 S.E.2d at 191.

135 No. 3:08-CR-0167-B 2009 WL 2356156, at *1 (N.D. Tex. July 9, 2009); *see also* Pell & Soghoian, *supra* note 8, at 119 (discussing this series of robberies).

136 Brian Owsley, *Cops and Robbers: The Use of Cell Tower Dumps to Investigate Bank Robberies*, American Criminal Law Review (Jan. 26, 2013, 16:40), http://www.americancriminallawreview.com/Drupal/blogs/blog-entry/cops-and-robbers-use-cell-tower-dumps-investigate-bank-robberies-01-26-2013-0. In a similar type of case involving a bank robbery, a "magistrate judge approved the request: 'The FBI was trying to find a bank robber. The robbery was [in a specific state], and they were pretty sure the robber and accomplices were from [a specific city]. They knew he had a cell phone. They asked for tower dumps to try to locate only phones with a [specific] area code which were in the immediate vicinity at the time of the robbery.'" *Id.*

137 *Duffey*, 2009 WL 2356156 at *1; *see also* Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET (Feb. 11, 2010, 4:00 AM PST), http://news.cnet.com/8301-13578_3-10451518-38.html ("FBI agents obtained logs from mobile phone companies corresponding to what their cellular towers had recorded at the time of a dozen different bank robberies in the Dallas area. The voluminous records showed that two phones had made calls around the time of all 12 heists, and that those phones belong to men . . . [who were] eventually convicted . . . of multiple bank robbery and weapons charges.").

138 *Duffey*, 2009 WL 2356156 at *2.

139 *Id.*

robbers."[140] Of course, just because cell tower dumps are rare does not mean that the manner in which this one was done passes constitutional muster.

C. Federal Court in Texas: Applications for Cell Tower Dumps

In the United States District Court for the Southern District of Texas, an Assistant United States Attorney filed an application on behalf of the United States of America for a court order of disclosure of telecommunications records in July 2011.[141] "That application sought to require AT&T, Cricket, Sprint/Nextel, T-Mobile, and Verizon Wireless to provide the FBI with cell phone records for four specific locations."[142] "Each location was identified by the address of a bank with a specific date and a fifteen minute interval."[143] "The [A]ssistant United States Attorney certified that the FBI was investigating multiple bank robberies and made the request pursuant to 18 U.S.C. § 2703(c) and (d)."[144] Ultimately, a court order was never granted regarding this application because the Assistant United States Attorney withdrew the application instead of responding to the magistrate judge's questions regarding the appropriate standard for the electronic surveillance request.[145]

In a series of three nearly identical applications filed also in the United States District Court for the Southern District of Texas, the Assistant United States Attorney sought the disclosure of cell tower records pursuant to 18 U.S.C. § 2703(c) and (d) from AT&T, Sprint/Nextel, and Verizon Wireless respectively in December 2011. Each application provided specific coordinates for two locations along with a date and a time period for those locations.[146] Both state and federal law enforcement agencies carried out the investigation regarding two individuals allegedly involved in the trafficking of narcotics. There were also allegations of a robbery by these two individuals. Although the Government had cell phone numbers associated with both individuals charged with drug smuggling, the applicant

---

140 McCullagh, *supra* note 137.

141 Brian L. Owsley, *Cops and Robbers: The Use of Cell Tower Dumps to Investigate Bank Robberies*, A. CRIM. L. REV. (2013), http://www.americancriminallawreview.com/Drupal/blogs/blog-entry/cops-and-robbers-use-cell-tower-dumps-investigate-bank-robberies-01-26-2013.

142 *Id.*

143 *Id.*

144 *Id.*

145 *Id.* ("Indeed, the application was withdrawn and the case number reassigned to another action.").

146 A copy of each of these three applications is on file with the author.

sought the cell tower records to "help clarify the locations and individuals possibly involved" in the robbery.[147] Ultimately, because the Government was unable to provide the court with support for the position that such records should be released without establishing probable cause, the court never granted the order regarding the request for all cell tower records. Instead, an order regarding the release of records associated with the two known cell numbers was issued pursuant to § 2703.

D. Federal Court in Arizona: United States v. Capito

On March 12, 2010, the United States Attorney for the District of Arizona charged Ronald Capito and Joel Glore with eight counts of bank robbery.[148] The High Country Bandits, as they were known, conducted a number of bank robberies in rural areas throughout the state. Based on a number of similarities among these robberies, the FBI agent leading the investigation obtained a court order from a federal magistrate judge "for records of all mobile telephones that registered with cell towers closest to four of the more remote robbery locations on the dates of the robberies."[149] Based on this cell tower dump, the investigating agents received over 150,000 telephone numbers.[150] They believed, however

> that due to the vast difference in distance and time between the cell towers and the dates of the robberies . . . that it would be extremely unusual for a cell phone number to appear on two or more of the cell phone towers servicing the area of the bank on the exact robbery dates.[151]

A computer analysis of these 150,000 telephone numbers revealed a single telephone number that definitively appeared at three of the towers near the robbed banks.[152] Further analysis revealed that this cell phone made contact with another cell phone immediately before two of the robberies, and more importantly, that the second cell phone was also near two of the cell towers around the time of the bank robberies.[153] After the application of a § 2703(d) order, it was determined that this first cell phone belonged to defendant Ronald

---

147 *Id.* at 7.

148 Criminal Complaint, United States v. Capito at 2–3, 35 (D. Ariz. Mar. 12, 2010) (No. 3:10-CR-8050).

149 *Id.* at 12–13.

150 *Id.* at 13. Some of those numbers were attached as exhibits to court documents. It is unclear what, if anything, the Government has done with the vast majority of the information received regarding the 150,000 numbers.

151 *Id.* at 13–14.

152 *Id.* at 14.

153 *Id.*

Capito and that the second cell phone belonged to defendant Joel Glore.[154]

In response to the electronic surveillance, Capito filed a motion to suppress the evidence obtained from the court order authorizing the cell tower dump, most notably, his identification and location among the 150,000 cell phone records.[155] He argued that the investigating agent used the § 2703(d) order because he was unable to establish probable cause.[156] He argued that the scale of the disclosure based on a dragnet search of every phone within the relatively close proximity of each of the four crime sites extended beyond the scope of an order addressing the historical cell-site information of one phone.[157]

In response, the Government maintained that a § 2703(d) order is the appropriate basis for obtaining historical cell site information.[158] Next, it argued that even if the order was improper, there was no statutory suppression remedy.[159] Even if the defendant's cell phone were deemed to be a tracking device, a warrant was unnecessary, and a suppression remedy was still unavailable.[160] Finally, the Government asserted that the defendant does not have any suppression remedy pursuant to the Fourth Amendment.[161]

At a hearing regarding the motion to suppress, the defendant denied arguing that cell tower information can never be obtained and used, but argued instead that there must simply be probable cause.[162] The district judge suggested that "[t]here is very good reason to think that these were similar perpetrators because of the identical modus operandi. There was the geographic proximity and more than a hunch that cell phones were being used."[163] When the defense attorney asserted that Capito's phone "is a cell phone that's tracking loca-

---

154 *Id.* at 15.

155 Motion to Suppress, United States v. Capito, (D. Ariz. Nov. 24, 2010) (No. 3:10-CR-8050).

156 *Id.* at 9–11.

157 *Id.* at 14.

158 Gov't Response to Motion to Suppress at 6–10, United States v. Capito, (D. Ariz. Feb. 7, 2011) (No. 3:10-CR-8050).

159 *Id.* at 10–13. Although the court cites to 18 U.S.C. § 3117 addressing tracking devices, *id.*, the Stored Communications Act explicitly bars any suppression remedies. *See* 18 U.S.C. § 2708 ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."); *see also United States v. Ferguson*, 508 F. Supp. 2d 7, 10 (D.D.C. 2007) ("Even if Defendant was correct that the Government did not comply with the SCA, the statute does not provide for a suppression remedy.") (citations omitted).

160 *Id.* at 10–14.

161 *Id.* at 14–15.

162 Transcript of Hearing at 18, United States v. Capito (D. Ariz. Sept. 14, 2011) (No. 3:10-CR-8050).

163 *Id.* at 19.

tion," the judge responded that "[i]t's a cell phone that's transmitting its location by the action and choice of everybody who has a cell phone."[164] Ultimately, the trial judge denied the motion to suppress, concluding that the § 2703(d) standard was met, but he did not explain this position beyond his conclusion.[165]

E. Federal Court in Connecticut: United States v. Soto

The United States Attorney for the District of Connecticut indicted Luis Soto and his brother, Felix Soto, for a series of bank robberies. A federal magistrate judge had issued an order pursuant to § 2703(d) requiring cell phone companies to provide information, including cell site location data. Ultimately, federal investigators obtained 180 different telephone numbers, for which telephone service providers had to give to agents "all cell site tracking data and cell site locator information for all incoming and outgoing calls to and from the Target Numbers."[166]

In a motion to suppress, the defendant argued that the order authorizing the release of this information was done without demonstrating probable cause and that the Government should have obtained a warrant in order to secure this information.[167] In response, the Government argued that the Stored Communications Act does not provide a remedy based on suppression.[168] It further asserted that historical cell site information does not impact a privacy interest pursuant to the Fourth Amendment.[169]

---

164 *Id.* at 23.

165 *Id.* at 35.

166 Memorandum in Support of Motion to Suppress at 1, United States v. Soto, (D. Conn. May 18, 2010) (No. 3:09-CR-200). Indeed, at a minimum, all 180 telephone numbers were made publicly available. *Id.* at Ex. B; *see also* McCullagh, *supra* note 66 (providing a link to a list of the phone numbers tracked).

167 Memorandum in Support of Motion to Suppress, United States v. Soto, (D. Conn. May 18, 2010) (No. 3:09-CR-200); *see also* Pell & Soghoian, *supra* note 8, at 120 (discussing how the government obtained and used historical cell tower logs).

168 Government's Response To Defendant's Motion To Preclude Cell Phone Evidence at 9–10, United States v. Soto, (D. Conn. June 28, 2010) (No. 3:09-CR-200); *see also* 18 U.S.C. § 2708 (2006) ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for no constitutional violations of this chapter."). Various courts have determined that suppression of evidence is not a remedy available pursuant to the Stored Communications Act. *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) ("[V]iolations of the ECPA do not warrant exclusion of evidence."); United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998) ("[T]he Stored Communications Act does not provide an exclusion remedy.").

169 Government's Response to Defendant's Motion to Preclude Cell Phone Evidence at 13–21, United States v. Soto, (D. Conn. June 28, 2010) (No. 3:09-CR-200).

In a one-page order, the district judge denied the motion to suppress:

> The basic premise of the defendant's motion is that the government did not obtain cell site location information by means of a warrant based upon a showing of good cause. This issue is addressed extensively in *In re Application of the U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010), where the court rejected the position being advocated by the defendant, and the court finds the analysis persuasive.[170]

The Third Circuit decision upon which the district judge relied does not address the suppression of evidence for any purported violations of the Stored Communications Act. Similarly, it does not cite to § 2708. Instead, that court held "that CSLI [Cell Site Location Information] from cell phone calls is obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination."[171] However, a magistrate judge (and presumably a district judge) has "the option to require a warrant showing probable cause" rather than the lesser standard.[172]

At trial in *Soto*,

> [t]he government presented the testimony of an expert in cellular site technology who used these cell site records to produce maps and charts showing that the participants in the robbery called one another extensively around the time of the robbery, while utilizing cellular towers within a short distance from [the bank].[173]

Ultimately, the defendant was convicted and sentenced to a lengthy term of incarceration.

F. Canadian Court in Ontario: Regina v. Mahmood

In *Regina v. Mahmood*, the Ontario Superior Court of Justice addressed a number of surveillance issues stemming from several warrants, including cell tower dumps. On November 17, 2006, in Brampton, Ontario, a suburb of Toronto, three men robbed a jewelry store of about $35,000 in cash and $500,000 in jewelry.[174] Initially, two

---

170 Order *re* Motion To Suppress Cell Site Location Information, United States v. Soto, (D. Conn. April 13, 2011) (No. 3:09-CR-200).

171 *Third Circuit Order*, 620 F.3d 304, 313 (3d Cir. 2010).

172 *Id.* at 319.

173 Press Release, U.S. Attorney's Office District of Connecticut, Federal Jury Finds Suffield Man Guilty of Robbing Berlin Bank (May 6, 2011), *available at* http://www.justice.gov/usao/ct/Press2011/20110506-2.html.

174 R. v. Mahmood, 2008 O.J. No. 3922, 236 C.C.C. 3d 3, 79 W.C.B. 2d 366 at ¶ 1, (Can. Ont. Sup. Ct. J. 2008), *aff'd* 2011 CanLII 693 (Can. Ont. C.A. 2011); *see also* QMI Agency, *'Burka' Bandit Denied Bail*, TORONTO SUN (Apr. 15, 2012, 5:27 PM, updated Apr. 15, 2012, 5:33 PM), http://www.torontosun.com/2012/04/15/burka-bandit-denied-bail.

men were buzzed into the store, one of them wearing a burqa as if he were the wife of the other man.[175] They then held the store owner at gunpoint and let in the third robber after applying duct tape to the store owner's eyes, mouth, and hands.[176]

With the exception of a plastic shopping bag from an Islamic fashion clothing store, the police had no evidence or leads to any suspects, but they suspected that the robbers used cell phones to perpetrate the heist.[177] Accordingly, police officers obtained several search warrants, including one for a Tower Records Dump for four different telecommunications providers.[178] On November 30, 2006, an officer swore "that 'as a robbery investigator with the Central Robbery Bureau', he was 'aware that cellular cell telephones are commonly being used as a means of communications by culprits committing robberies,' and that tower dumps had been helpful to the police in the past."[179] This warrant "required that [these providers] produce all records of all cellular phone traffic that had passed through two cellular towers located in the vicinity of the crime for the hour and a half that preceded the robbery."[180] That warrant ultimately yielded more than 7,000 different cell phone subscribers, including two of the defendants in the robbery.[181] Based on this information, investigators obtained several more warrants.

Before the trial court, the defendants argued that the Tower Dump Warrants violated their rights pursuant to the Canadian Charter of Rights and Freedoms.[182] Specifically, they asserted that their right to privacy had been violated. The court concluded that the defendants had a reasonable expectation of privacy in their cell phone records.[183] The court was deeply troubled by these warrants:

---

175 QMI Agency, *supra* note 174.

176 *Mahmood*, 2008 CanLII 51774 (ON SC), 2008 O.J. No. 3922, 236 C.C.C. (3d) 3, 79 W.C.B. 2d 366 at ¶ 1.

177 *Id.* at ¶¶ 1–2, 10, 12.

178 *Id.* at ¶ 2–3.

179 *Id.* at ¶ 92.

180 *Id.* at ¶ 3; *see also id.* at ¶ 14 ("They wanted all records for all cellular telephone traffic that had passed through those transmission towers, owned by Rogers Wireless, Fido, Bell Mobility and Telemobile, for November 17, 2006 between 10:20 a.m. and 11:50 a.m., just prior to the robbery.").

181 *Id.* at ¶ 3.

182 *Id.* at ¶ 40; *see also* Canadian Charter of Rights and Freedoms, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act, 1982, c. 11 (U.K.) [hereinafter Canadian Charter of Rights and Freedoms], § 8 ("Everyone has the right to be secure against unreasonable search or seizure.").

183 *See Mahmood*, CanLII 51774 (ON SC), 2008 O.J. No. 3922, 236 C.C.C. 3d 3, 79 W.C.B. 2d 366 at ¶¶ 55–82; *see generally* Teresa Scassa, *Information Privacy in Public Space: Location Da-*

> Most importantly here, the police did not obtain such information under the Tower Dump Warrants for known or named individuals or known or named cell phone numbers. They had no knowledge of any particular person who may have used a cell phone in that vicinity on that day, and did not channel their search or focus it on any individual persons until they obtained the second warrant for the Subscriber Records for several of these four Applicants. It is disingenuous to suggest that the initial Tower Dump Warrants were any more than a high-tech "fishing expedition" of the broadest order made in the hope that some information would be obtained that would permit the police investigation to move forward.[184]

Regarding these warrants, it concluded that the lack of focus regarding the search was objectively unreasonable because the investigators received access to the records of more than 7000 persons merely because an officer swore that in his experience, cell phones are frequently used in robberies.[185]

Next, the court concluded that the police did not have reasonable or probable grounds to obtain these warrants.[186] The court characterized the Tower Dump Warrants as an impermissible fishing expedition.[187] Ultimately, the trial judge determined that the warrants violated the rights of thousands of people, including the defendants.[188] Next, he considered whether the evidence obtained from this warrant was admissible at the defendants' trial.[189] Ultimately, he concluded that the Canadian Charter of Rights and Freedoms required the exclusion of the evidence "to clearly and unequivocally convey to police authorities that Canadian citizens have the constitutional right to be left alone from this kind of unwarranted and unfocused state intrusion into their daily lives."[190]

Notwithstanding the exclusion of evidence from the Tower Dump Warrants, a jury convicted the defendants of several offenses related

---

ta, Data Protection and the Reasonable Expectation of Privacy, 7 CAN. J. L. & TECH. 193 (2010) (discussing *Mahmood* and the privacy concerns raised by the police investigation).

184 *Mahmood*, 2008 CanLII 51774 (ON SC), 2008 O.J. No. 3922, 236 C.C.C. (3d) 3, 79 W.C.B. 2d 366 at ¶ 72.

185 *Id.* at ¶ 78.

186 *See id.* at ¶¶ 83–100.

187 *Id.* at ¶¶ 85, 94.

188 *Id.* at ¶ 95.

189 *See id.* at ¶¶ 103–22.

190 *Id.* at ¶ 121; *see also* Canadian Charter of Rights and Freedoms, § 24(2) ("Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.").

to the robbery.[191] The Court of Appeals for Ontario affirmed the convictions.[192]

VI. CELL TOWER DUMPS SHOULD NOT BE ANALYZED OR GRANTED PURSUANT TO § 2703

As various courts have addressed, improving technology enables the recipients of cell site location information to pinpoint a cell phone within about one hundred feet or less.[193] At the end of 1986, the year Congress enacted the Electronic Communications Privacy Act, there were only 1531 cell sites throughout the United States.[194] At the end of 2011, there were 283,385 cell sites throughout the United States, up from 127,540 at the end of 2001.[195] As the number of cell towers increases, the accuracy of the tracking of a specific cell phone (and the cell phone's user) vastly improves.[196] This enhanced tracking accuracy is further improved by the increased use of femtocells and picocells.[197] Similarly, in *United States v. Jones*, the Supreme Court noted that "[b]y means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer."[198]

---

191 R. v. Mahmood, 2011 CanLII 693 at ¶ 4 (Can. Ont. C.A., 2011).

192 *See generally id.*

193 *Eastern New York Order 2*, 736 F. Supp. 2d 578, 590 n.14 (E.D.N.Y. 2010) ("As of February 2008, CSI from multiple towers could reveal the location of a cell phone to within approximately 50 feet, and information from a single tower to within a few hundred feet." (citing *In re* Application of U.S. for an Order Directing a Provider of Electronic Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 602 (W.D. Pa. 2008)); *Southern Texas Order 2*, 747 F. Supp. 2d 827, 833 (S.D. Tex. 2010) ("By correlating the precise time and angle at which a phone's signal arrives at multiple sector base stations, a provider can pinpoint the phone's latitude and longitude to an accuracy within 50 meters or less. Emerging versions of the technology are even more precise." (citation omitted)); *Western Texas Order*, 727 F. Supp. 2d 571, 580 (W.D. Tex. 2010) ("Estimates from three years ago [2007] were that over 90% of cell phones then in use had GPS capabilities, through which the target phone could be located to within as little as 50 feet." (citation omitted)); *see also* Pell & Soghoian, *supra* note 8, at 127 ("[T]he proximity of one cell site to another in a geographic area is one factor in the production of more accurate location data.").

194 CTIA-The Wireless Association, Annualized Wireless Industry Survey Results—December 1985 to December 2011 (2012), http://www.files.ctia.org/pdf/CTIA_Survey_Year_End_2011_Graphics.pdf.

195 *Id.*

196 *See* In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers, 402 F. Supp. 2d 597, 599 n.4 (D. Md. 2005).

197 *See supra* note 12 and accompanying text.

198 132 S. Ct. 945, 948 (2012).

A. *The Decision in* United States v. Jones *Foreshadows a New Heightened Awareness of the Fourth Amendment Implications for Twenty-First-Century Surveillance Technology*

In *United States v. Maynard*, during a narcotics trafficking investigation, the government employed various methods of surveillance, including installing a GPS device on the defendant Antoine Jones's vehicle, which in part led to his conviction.[199] That GPS device tracked Jones's "movements 24 hours a day for 28 days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place to place."[200]

The United States Court of Appeals for the District of Columbia held that by tracking the defendant Jones's movements everywhere for a month, the warrantless GPS application to Jones's car constituted a search because it defeated his reasonable expectations of privacy.[201] In so doing, the court expressed grave concerns about the invasive nature of the GPS surveillance.[202]

After granting certiorari,[203] the Supreme Court further elaborated that the government received a warrant from the United States District Court for the District of Columbia that authorized the GPS tracking device on the defendant's vehicle *provided* that it was installed in the District of Columbia within ten days of the court order.[204] However, the agents installed the GPS tracking device in Maryland one day after the order authorizing it expired.[205] As a result of this surveillance, "the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2000 pages of data over the 4-week period."[206]

---

199 615 F.3d 544, 549, 555 (D.C. Cir. 2010), *aff'd* United States v. Jones, 132 S. Ct. 945 (2012).

200 *Maynard*, 615 F.3d at 558; *see also* Fabio Arcila, Jr., *GPS Tracking out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1, 13 (2012) (addressing the application in *Maynard* of the mosaic theory as "controversial because it suggests that some limited degree of warrantless GPS tracking would be constitutional under the Fourth Amendment, but too much is not").

201 *Maynard*, 615 F.3d at 555–66; *see also* People v. Weaver, 909 N.E.2d 1195, 1199–1200 (N.Y. 2009) ("What the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits.").

202 *Maynard*, 615 F.3d at 562–63.

203 *United States v. Jones*, 131 S. Ct. 3064 (2011).

204 *Jones*, 132 S. Ct. at 948.

205 *Id.*

206 *Id.*

In the majority opinion, Justice Antonin Scalia began by framing his analysis in the historical language of trespass.[207] He then discussed the common law trespass approach, citing to *Olmstead* before acknowledging the reasonable expectation of privacy approach developed in *Katz*.[208] He continued by explaining that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."[209] He distinguished the Court's decision in *United States v. Karo* because the container with the tracking device was not originally in that defendant's possession when the surveillance tool was inserted into the container, whereas Jones always had a possessory interest in his vehicle.[210] Thus, the Court held that the installation and use of the GPS to monitor Jones's movements constituted a search in violation of the Fourth Amendment.[211]

In a concurrence, Justice Samuel Alito, joined by Justices Ruth Bader Ginsburg, Stephen Breyer, and Elena Kagan, lambasted the trespass theory espoused by Justice Scalia's majority opinion.[212] Instead, he promoted the reasonable expectation of privacy approach developed in *Katz* and its progeny, maintaining that that decision "finally did away with the old approach, holding that a trespass was not required for a Fourth Amendment violation."[213] The *Katz* test provides the flexibility to adapt to new technologies and ensure that privacy interests are protected.

Finally, Justice Sonia Sotomayor issued a concurring opinion acknowledging that the Fourth Amendment may be concerned "with trespassory intrusions on property."[214] However, she also recognized that "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion of property, the majority opinion's trespassory test may provide little guidance."[215] In supporting both the majority's trespassory approach as well as the reasonable expectation of privacy from *Katz*, she calls into question the line of

---

207 *Id.* at 949.

208 *Id.* at 949–50.

209 *Id.* at 952 (emphases in original); *see also* Arcila, *supra* note 200, at 14 (noting that the *Katz* conundrum centered on whether the Court meant "to replace property with privacy, or merely to supplement property with privacy"). At least for Justice Scalia, it is the latter. *See id.* at 69 ("Justice Scalia's approach holds the promise of expanding Fourth Amendment protections by doubling the conceptual bases upon which such safeguards can be claimed.").

210 *Jones*, 132 S. Ct. at 952 (discussing United States v. Karo, 468 U.S. 705, 707, 712 (1984)).

211 *Id.* at 949.

212 *Id.* at 957–58 (Alito, J., concurring).

213 *Id.* at 959 (Alito, J., concurring).

214 *Id.* at 954 (Sotomayor, J., concurring).

215 *Id.* at 955 (Sotomayor, J., concurring).

cases emanating from *Smith v. Maryland* that indicated that individuals have no privacy interest in information accessible to third parties such as telecommunications providers. Specifically, she characterized "[t]his approach [as] ill suited to the digital age," calling for an end to "treat[ing] secrecy as a prerequisite for privacy."[216]

In *Jones*, the Supreme Court muddled the development of the already hazy Fourth Amendment jurisprudence.[217] Yet, it is clear that the Court—based on a unanimous judgment—provides the message that individual privacy rights remain strong concerning new surveillance technologies.[218] Indeed, with the myriad theories espoused by the Justices, individuals now may raise several arguments to support heightened standards to protect individual privacy rights in their location data.

B. Recent Developments in Technology Establish that Probable Cause Is Required Where Cell Site Data Establish a Cell Phone User's Location Information

It is understandable that law enforcement officials would favor seeking approval for a cell tower dump based on the "specific and articulable facts" standard because it is easier to satisfy than establishing probable cause. In seeking to apply the "specific and articulable facts" standard, many courts have rejected arguments that probable cause and the Fourth Amendment must be applied to requests for

---

216 *Id.* at 955, 957 (Sotomayor, J., concurring).

217 *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (addressing the potential emergence of a "mosaic theory" of the Fourth Amendment where a search is established based on an approach of aggregating government action); *see also* Arcila, *supra* note 199, at 50–64 (discussing the use of the mosaic theory in the context of GPS tracking and the resulting debate regarding this approach).

218 *See* Arcila, *supra* note 199, at 17 ("[E]ach of the three opinions produced in *Jones* holds the potential to be important in the future development of Fourth Amendment jurisprudence.").

historical cell site data.[219] Other courts have determined that probable cause is necessary for such information.[220]

In discussing the appropriate standard, District Judge Nicholas Garaufis explained that a request for cell site information raises a greater concern than a request for a tracking device on a vehicle:

> The cell-site-location records at issue here currently enable the tracking of the vast majority of Americans. Thus, the collection of cell-site-location records effectively enables "mass" or "wholesale" electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip. This further supports the court's conclusion that cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location records and that the Government's obtaining these records constitutes a Fourth Amendment search.[221]

Similarly, Magistrate Judge Andrew Austin has explained that there is a problem with the government's approach to surveillance using cell site data: "The probable cause affidavit for CSLI rarely suggests that every activity in the target's life is illegal activity, yet receipt of CSLI will permit the government to 'follow' the phone user's movements 24 hours a day, 7 days a week, wherever they go, whatever they are doing."[222] Consequently, he concluded that the appropriate course is to "insist on strict adherence to the requirements of Rule 41 on all requests for CSLI, including requests for historical data. The warrants will be granted only on a showing of probable cause . . . ."[223]

---

219 United States v. Graham, 846 F. Supp. 2d 384, 388–389 (D. Md. 2012); United States v. Benford, No 2:09CR86, 2010 WL 1266507, at *2–*3 (N.D. Ind. 2010); *In re* Applications of U.S. for Orders Pursuant To Title 18, U.S. Code Section 2703(d), 509 F. Supp. 2d 76, 80–81 (D. Mass. 2007) (*reversing In re* Applications of U.S. for Orders Pursuant To Title 18, U.S. Code Section 2703(d) to Disclose Subscriber Information and Historical Cell Site Information, 509 F. Supp. 2d 64 (D. Mass. 2007), in which a magistrate judge held that probable cause was required for the disclosure of historical cell site information); *see also* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 16, at 41 ("Law enforcement investigators may use a search warrant or an order under section 2703(d) of title 18 in order to obtain historical records from cellular carriers.").

220 *Eastern New York Order 1*, 809 F. Supp. 2d 113, 125 (E.D.N.Y 2011); *Southern Texas Order* 2, 747 F. Supp. 2d 827, 837–40 (S.D. Tex. 2010); *Western Texas Order*, 727 F. Supp. 2d 571, 583–84 (W.D. Tex. 2010); *Western Pennsylvania Order*, 534 F. Supp. 2d 585, 616 (W.D. Pa. 2008); *In re* Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information, No. 10-MC-0897, 2010 WL 5437209, at *4 (E.D.N.Y. Dec. 23, 2010); *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), Nos. C-12-755M, C-12-756M, C-12-757M, 2012 WL 3260215, at *2 (S.D. Tex. July 30, 2012). In the interest of full disclosure, this latter decision is one that I issued.

221 *Eastern New York Order 1*, 809 F. Supp. 2d at 119–20.

222 *Western Texas Order*, 727 F. Supp. 2d at 582.

223 *Id.* at 583–84; *see also* Freiwald, *supra* note 65, at 691 n.65 (addressing the application of Rule 41 and arguing that obtaining historical cell site location data is a search pursuant to the Fourth Amendment).

Finally, Magistrate Judge Stephen Smith addressed a government application for historical cell site information. First, he noted that "new technology has altered the legal landscape even more profoundly than the new case law."[224] Based on these developments in technology, he explained that "court decisions allowing the Government to compel cell site data without a probable cause warrant were based on yesteryear's assumption that cell site data (especially from a single tower) could locate users only imprecisely."[225] Analyzing *Maynard*, he determined that historical cell site data was subject to Fourth Amendment protections.[226] After distinguishing *Smith v. Maryland*, Judge Smith concluded that prolonged surveillance barred an order for two months of cell site location records unless a warrant was obtained.[227]

On appeal pursuant to 28 U.S.C. § 636, District Judge Lynn Hughes overruled the Government's objections, explaining that "[w]hen the government requests records from cellular services, data disclosing the location of the telephone at the time of particular calls may be acquired only by a warrant issued on probable cause."[228] In the applications before the court, because the requested "records would show the date, time, called number, and location of when the call was made," this information was "constitutionally protected from this intrusion."[229] Most significantly, Judge Hughes concluded that "[t]he standard under the Stored Communications Act, 18 U.S.C. § 2703(d), is below that required by the Constitution."[230] As historical cell site data would reveal an individual's location, such intrusion by the government constitutes a search requiring a showing of probable cause.

The Government appealed the order upholding Judge Smith's denial of the application as well as Judge Hughes' order. In a recent decision with a divided panel, the Fifth Circuit reversed the district

---

224 *Southern Texas Order 2*, 747 F. Supp. 2d at 830; *see also* Pell & Soghoian, *supra* note 8, at 145 (discussing Judge Smith's opinion).

225 *Southern Texas Order 2*, 747 F. Supp. 2d at 837 (citation omitted).

226 *Id.* at 838–40.

227 *Id.* at 846.

228 Order on Objections, *In re* Applications of the U.S. for Historical Cell Site Data, Misc. (S.D. Tex. Nov. 11, 2011) (No. H-11-223) (citing U.S. CONST. amend. IV).

229 *Id.*

230 *Id.* The Government has appealed the order upholding Judge Smith's denial of the application. *See In re* United States for Historical Cell Site Data, *appeal docketed*, No. 11-20884 (5th Cir. Dec. 14, 2011). Any decision by the Fifth Circuit may provide guidance on some issues regarding cell site data and surveillance, but will not address cell tower dumps.

court.[231] The majority opinion initially concluded that it could not avoid the constitutional question addressed by the district court.[232] Ultimately, the Fifth Circuit determined that the production of historical cell site records that were maintained as business records by the telecommunications providers was not per se unconstitutional.[233]

In a dissenting opinion, one circuit judge expressed dismay at the majority's opinion, noting that it was not only incorrect, but it created a circuit split on two issues with the Third Circuit.[234] He took issue with the majority's conclusion that a magistrate must issue a § 2703(d) order whenever the Government satisfies the "reasonable and articulable" standard.[235] Significantly, the dissenting judge argued that the statute was ambiguous as to when a warrant should be required.[236] Because the dissenting judge "concluded that the statute is best construed as directing that warrant procedures be followed when the government seeks non-consent records that may be protected by the Fourth Amendment," he would have held "that historical cell site location records constitute one example of this potentially protected information," and thus, a warrant should be obtained.[237]

In the end, the majority opinion noted that the issue decided was a narrow one: "Section 2703(d) order to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional."[238] Specifically, the court further explained that the decision does not address, among other issues, applications "requesting data from all phones that use a tower during a particular interval," or for requests of "location information for the duration of the calls or when the phone is idle."[239] In other words, the court explicitly indicated that the decision did not address cell tower dumps. Moreover, the decision does not apply where the government would seek the cell site lo-

---

231 *See generally In re* Application of U.S. for Historical Cell Site Data, No. 11-20884, 2013 WL 3914484 (5th Cir. July 30, 2013).

232 *Id.* at *6.

233 *Id.* at *8–12.

234 *Id.* at *13 (Dennis, J., dissenting) (citing *Third Circuit Order*, 620 F.3d 304, 315–17 (3d Cir. 2010)).

235 *Id.* at *16 (Dennis, J., dissenting) ("[A] showing of reasonable suspicion clearly is a necessary condition for the issuance of a § 2703(d) order, but not a sufficient condition. Contrary to the assertions of the government and the majority, nowhere does the statute by its terms *require* a court to issue a § 2703(d) order whenever the government's application demonstrates reasonable suspicion.").

236 *Id.* at *18 (Dennis, J., dissenting).

237 *Id.* at *24.

238 *Id.* at *12 (majority opinion).

239 *Id.*

cation data of cellphones even when they are not being used to make or receive calls.

With the circuit split and numerous decisions at the district court level, there is still significant support for requiring probable cause for historical cell site data. This requirement is especially true where the government is seeking prospective cell site location information or similar data for all times when the cell phone is turned on but not engaged in a telephone call.[240]

C. There Are a Number of Issues with the Government's Approach to Cell Tower Dumps that Call for Reconsideration and Reform

When seeking a cell tower dump, the government typically files an application using its one-size-fits-all form to obtain the specific order regarding electronic surveillance sought in a given investigation. Indeed, the Department of Justice provides its Assistant United States Attorneys with a form application for a § 2703(d) court order as well as form order approving the application that they are to file with the court seeking any relief pursuant to § 2703(d).[241] Often, the Assistant United States Attorney filing the application seeking an order for some kind of sophisticated electronic surveillance does not understand the technology and has difficulty explaining it or responding to questions regarding its operation.[242] Similarly, the case agents typically do not understand how the surveillance equipment works. Apparently, they rely on a few agents and consultants around the country who often testify as experts regarding this form of electronic surveillance.[243]

Further compounding the problem is that the government's applications are, as a matter of course, filed ex parte under seal. Of course, it is important that these applications be filed under seal.[244]

---

240 *See, e.g.*, *Western Texas Order*, 727 F. Supp. 2d 571, 582 (W.D. Tex. 2010) (discussing applications requesting around-the-clock-cell site location information).

241 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 16 at 162–65.

242 *See, e.g.*, *In re* Application of U.S. for An Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012). In the interest of full disclosure, this decision is one that I issued.

243 *In re* United States *ex rel.* Order Pursuant to 18 U.S.C. Section 2703(d), Nos. C-12-670M, C-12-671M, C-12-672M, C-12-673M, 2012 WL 4717778, at *1 (S.D. Tex. Sept. 26, 2012). Of course, this lack of understanding may stem from an attempt by law enforcement to avoid acknowledging the use of sensitive electronic surveillance techniques. *See, e.g.*, Pell & Soghoian, *supra* note 8 at 158.

244 Catherine Crump & Christopher Calabrese, *Location Tracking: Muddled and Uncertain Standards Harm Americans' Privacy*, 88 CRIM. L. REP. 19, 21 (2010) ("For legitimate reasons, applications to track cell phones are often filed under seal. Law enforcement agents sometimes need to prevent the targets of government surveillance from learning that

Nonetheless, even magistrate judges have a difficult time ascertaining how other judges are addressing these issues. Instead, we must rely on word-of-mouth and caucusing with various colleagues. In applying this approach, for example, I did not receive any responses from the magistrate judges involved in *Capito*, *Duffey*, or *Soto*.

Notwithstanding the debate within the federal courts about what standard applies for historical cell site data, the "specific and articulable facts" standard is more problematic concerning cell tower dumps given the volume of information that law enforcement officials receive.[245] However, as the Supreme Court's decision in *Jones* demonstrates, law enforcement agents who use electronic surveillance should avoid pushing the envelope, as it just takes one decision to adversely impact a significant number of criminal prosecutions.[246] It is quite likely that there are a number of prosecutors and law enforcement officials scrambling post-*Jones* to ensure that convictions are not jeopardized or overturned.[247] Indeed, as a result of *Jones*, the

---

they are investigative subjects."); *see also* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 315 (2012) ("Of course, some measure of temporary secrecy for electronic surveillance orders during a criminal investigation is both reasonable and necessary. Premature disclosure to the target or the general public could jeopardize the integrity of the ongoing investigation and encourage the target to flee or destroy evidence.").

245 *See* Mary Graw Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L.J. 1035, 1087 (2011) ("[S]uch a low standard, combined with technological vulnerabilities and volume of information, may create the unintended consequence of a loss of protections for [private information]."). Of course, law enforcement officials typically favor this lower standard because "procuring a search warrant, based on probable cause, is too time-consuming and slows down an investigation." Somini Sengupta, *For Congress, a Question of Cellphone Tracking*, N.Y. TIMES (Apr. 25, 2013, 11:22 AM), http://bits.blogs.nytimes.com/2013/04/25/for-congress-a-question-of-cellphone-tracking/.

246 *See* Michael E. Horowitz & April Oliver, *Foreword: The State of Federal Prosecution*, 43 AM. CRIM. L. REV. 1033, 1040 (2006) ("[A] mega-trend affecting the federal landscape [of an area of criminal law] stems from one case."); Christopher B. Mueller, Daubert *Asks the Right Questions: Now Appellate Courts Should Help Find the Right Answers*, 33 SETON HALL L. REV. 987, 988 (2003) ("[A] single case so profoundly changes the legal landscape.").

247 *See, e.g.*, United States v. Cuevas-Perez, 640 F.3d 272 (7th Cir. 2011) (holding that the placement of a GPS tracking unit on a defendant's car did not violate the Fourth Amendment), *vacated* Cuevas-Perez v. United States, 132 S. Ct. 1534 (2012) (remanding "for further consideration in light of United States v. Jones"); United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010) ("[T]he police did not conduct an impermissible search of Pineda-Moreno's car by monitoring its location with mobile tracking devices."), *vacated* Pineda-Moreno v. United States, 132 S. Ct. 1533 (2012) (remanding "for further consideration in light of United States v. Jones"). On remand in *Pineda-Moreno*, the Ninth Circuit upheld his conviction because there was other evidence that supported the traffic stop and, ultimately, the conviction. United States v. Pineda-Moreno, 688 F.3d 1087, 1089–91 (9th Cir. 2012). However, in *Cuevas-Pineda*, the trial court granted the Government's motion to dismiss the indictment. United States v. Cue-

FBI General Counsel reported that his agency "turn[ed] off about 3,000 GPS tracking devices that were in use."[248]

This new surveillance technology cannot be ignored. Moreover, other technological developments are sure to follow. However, the use of the specific and articulable standard to support the use of cell tower dumps is, at best, ill-advised. Ideally, Congress would enter the debate and provide a statutory basis consistent with the Constitution. The longer that Congress waits to provide new legislation, the more outdated the present statutes become regarding the various new developments in electronic surveillance. Unfortunately, Congress seems loath to initiate any legislation, including that which addresses electronic surveillance. As scholars have noted, "Historically, Congress has dragged its heels in protecting communications privacy until the courts have demanded it."[249] Indeed, the governors of Rhode Island and California have rejected legislation regarding surveillance of cell phones.[250]

---

vas-Perez, No. 4:09-CR-40009 (S.D. Ill. Jan. 18, 2013). Similarly, district courts have also suppressed evidence from warrantless GPS searches based on *Jones*. *See* United States v. Ortiz, 878 F. Supp. 2d 515, 526–43 (E.D. Pa. 2012) (finding that the warrantless search required the exclusion of evidence obtained from the GPS); United States v. Lee, 862 F. Supp. 2d 560, 570–71 (E.D. Ky. 2012) (adopting the magistrate judge's recommendation to suppress the evidence from a warrantless GPS search); *see also* United States v. Lee, No. 6:11-CR-65, 2012 WL 1880636 (E.D. Ky. Mar. 22, 2012) (report and recommendation). Finally, state courts have also suppressed evidence obtained from warrantless GPS searches; *see generally* State v. Zahn, 812 N.W.2d 490 (S.D. 2012) (reversing and remanding based on *Jones*); State v. Johnson, 964 N.E.2d 426 (Ohio 2012) (vacating conviction and remanding in light of *Jones*); State v. Winningham, 969 N.E.2d 251 (Ohio 2012) (same); State v. Sayles, 969 N.E.2d 251 (Ohio 2012) (same); State v. Jefferson, 969 N.E.2d 250 (Ohio 2012) (same); State v. Sullivan, 969 N.E.2d 250 (Ohio 2012) (same); State v. White, 969 N.E.2d 243 (Ohio 2012) (same); People v. Robinson, 269 P.3d 653 (Cal. 2012) (same).

248 Julia Angwin, *FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling*, WALL ST. J. (Feb. 25, 2012, 3:36 PM), http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling; *accord* Arcila, *supra* note 199, at 5.

249 Freiwald, *supra* note 65, at 687; *see also* Bankston, *supra* note 69, at 631 (calling for Congress to update the Stored Communications Act); *Western Texas Order*, 727 F. Supp. 2d 571, 573 (W.D. Tex. 2010) ("As technology has advanced, new investigative tools have become available that federal law does not explicitly address."). *But see* Kerr, *supra* note 50, at 858–59 ("Courts lack the institutional capacity to easily grasp the privacy implications of new technologies they encounter. Judges cannot readily understand how the technologies may develop, cannot easily appreciate context, and often cannot even recognize whether the facts of the case before them raise privacy implications that happen to be typical or atypical. Judicially created rules also lack necessary flexibility; they cannot change quickly and cannot test various regulatory approaches."). Indeed, in 2000, the House Judiciary Committee fashioned a bill regarding the standards for prospective cell site location data, but that bill ultimately died. Pell & Soghoian, *supra* note 8, at 159–60.

250 *See, e.g.*, Hanni Fakhoury, *Governor Brown Vetoes California Electronic Privacy Protection. Again.*, ELECTRONIC FRONTIER FOUND. (Oct. 1, 2012), https://www.eff.org/

In the absence of new legislation with standards specifically addressing cell tower dumps, courts must address the issues. As Professor Orin Kerr has argued, "[c]hanging technology can outpace the assumptions of existing precedents, and courts may need to tweak prior doctrine to restore the balance of privacy protection from an earlier age."[251] Of course, technology can change so dramatically that existing statutes may no longer adequately address privacy concerns. Moreover, if Congress were to enact new legislation regarding electronic surveillance, then "every reasonable construction must be resorted to in order to save a statute from unconstitutionality."[252] However, courts may not find any such new laws constitutional if the standard for electronic surveillance intruding upon a reasonable expectation of privacy is less than the issuance of a warrant based on a probable cause standard. Congress can create any standard it likes, but whatever standard it creates, it will eventually be subjected to judicial review and must pass constitutional muster.[253]

In discussing requests for court orders, warrants, and subpoenas with various case agents, I always stressed that denying orders that fail to satisfy the standard is not just doing right by the Constitution and the applicable statutes, but also benefiting society as well.[254] These agents do not want to have a conviction hinge on—and potentially be overturned—because of an order or warrant that does not satisfy the standard.[255] This argument has been made easier by the Supreme Court's decision in *Jones*, because some agents are now furiously working to determine what, if anything, they need to do to salvage

---

deeplinks/2012/10/governor-browns-vetoes-california-electronic-privacy-protection-again; Somini Sengupta, *Courts Divided over Searches of Cellphones*, N.Y. TIMES, Nov. 26, 2012, at A1 (Governor Lincoln Chafee vetoed a bill that would have compelled police to obtain a warrant to search a cell phone).

251 Kerr, *supra* note 216, at 344.

252 *See, e.g.*, Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council, 485 U.S. 568, 575 (1988) (quoting Hooper v. California, 155 U.S. 648, 657 (1895)); Gonzales v. Carhart, 550 U.S. 124, 153 (2007) (quoting *Edward J. DeBartolo Corp.*, 485 U.S. at 575).

253 *See* Coolidge v. New Hampshire, 403 U.S. 443, 454 (1971) ("It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon." (citing Boyd v. United States, 116 U.S. 616, 635 (1886)).

254 *See, e.g.*, Gerald S. Reamey, *When 'Special Needs' Meet Probable Cause: Denying the Devil Benefit of Law*, 19 HASTINGS CONST. L.Q. 295, 340 (1992) ("If the constitutional scheme requires probable cause and a warrant for searches designed to produce criminal evidence, it is hard to imagine what further societal need would be so significant that its presence should reduce the standard of suspicion and judicial review.").

255 *See, e.g.*, David J.R. Frakt, *Fruitless Poisonous Trees in a Parallel Universe:* Hudson v. Michigan*, Knock-and-Announce, and the Exclusionary Rule*, 34 FLA. ST. U. L. REV. 659, 698 (2007) ("[P]olice will adopt whatever tactics they can aggressively implement if they can increase their conviction rate and not be overturned on appeal . . . .").

cases involving a *Jones*-like search. Moreover, *Jones* has demonstrated that the courts are willing to act as a check on government investigations regarding electronic surveillance. That is particularly true because *Jones* was a unanimous judgment from a Court that routinely issues decisions split along ideological lines.[256]

In the absence of any legislative guidance from Congress, the courts must develop jurisprudence. As evident by the various cases, there are a significant number of decisions by magistrate judges as well as some district judges addressing § 2703. However, the government generally appears opposed to appealing adverse decisions to federal appellate courts—no doubt interested in avoiding creating bad case law. Consequently, with the exception of the Third Circuit and the Fifth Circuit decisions, there are no federal appellate decisions addressing historical cell site data and the standards to be applied.[257] Moreover, these are the only two appellate decisions in over eight years that these issues have been raised before district courts around the country. Given this slow pace, it is unlikely that there will be any new decisions soon, and even more unlikely that the Supreme Court will grant certiorari and issue a decision with definitive guidance on this issue. Indeed, the procedural posture of these ex parte applications makes it more unlikely that there will be any Supreme Court decisions.

Based on the Fourth Amendment and developing case law, requests for cell tower dumps should not be handled through applications pursuant to § 2703. The provision of location information invades numerous individuals' privacy rights. This is evident on remand in the *Jones* case, where the Government can no longer establish the defendant's whereabouts after the Supreme Court's *Jones* decision based on the defendant's GPS records, it subsequently sought to establish the defendant's location based on his cell site location data records.[258] Instead, requests for access to such information should be filed pursuant to Rule 41 of the Federal Rules of Criminal Procedure. Such a warrant must satisfy the probable cause standard based

256 *See* Mark R. Killenbeck, *William Johnson, The Dog That Did Not Bark?*, 62 VAND. L. REV. 407, 409 n.11 (2009) (noting media reports of frequent "5-to-4 decision splits along ideological lines" in recent years); Caren Myers Morrison, *The Drug Dealer, the Narc, and the Very Tiny Constable: Reflections on* United States v. Jones, 3 CALIF. L. REV. CIR. 113, 113–14 (2012) ("Although the Justices all agreed that the government's conduct amounted to a search, the reasoning of the case was hotly disputed.").

257 Because the Government prevailed before the Fifth Circuit in its ex parte application, there is no party to seek Supreme Court review even though there is a circuit split.

258 Kerr, *supra* note 216, at 322 n.72.

on the totality of the circumstances.[259] Indeed, to the extent that the information the government seeks constitutes a tracking device, a warrant is the appropriate manner in which judicial authorization for such a device is provided.[260]

In addition to satisfying the probable cause standard, applications for cell tower dumps should provide some safeguards for individuals who are not subjects of the criminal investigation whose personal information will nonetheless be gathered in the course of the dump. The Wiretap Act,[261] which authorizes wiretaps, provides some guidance.[262]

First, the statute not only requires a probable cause standard,[263] but also mandates that a wiretap should only be authorized after "normal investigative procedures have been tried and have or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[264] In other words, a cell tower dump should not be used as a big fishing expedition. This approach is "designed to assure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime."[265] In other words, wiretapping is an investigative approach that should be the last resort for law enforcement officials. Similarly, a cell tower dump can serve a useful purpose in criminal investigations, but it should be the last approach used after various other methods, including pen registers and trap and trace devices and orders issued pursuant to § 2703 as well as other non-electronic investigative techniques. For example, in the bank robbery scenario involving multiple crime scenes, the investigat-

---

259 Illinois v. Gates, 462 U.S. 213, 238 (1983); *accord* United States v. Settegast, 755 F.2d 1117, 1121 (5th Cir. 1985).

260 FED. R. CRIM. P. 41(e)(2)(C).

261 Pub. L. No. 90-351, 82 Stat. 197 (1968).

262 *See* Freiwald, *supra* note 65, at 747–48 (positing that the Wiretap Act protections should apply to historical cell site searches).

263 18 U.S.C. § 2518(3)(a) (1998) (wiretap may be authorized upon a showing of "probable cause for the belief that an individual is committing, has committed, or is about to commit a particular offense"); 18 U.S.C. § 2518(3)(b) (1998) (wiretap may be authorized upon a showing of "probable cause for the belief that particular communications concerning that offense will be obtained through such interception"); 18 U.S.C. § 2518(3)(d) (wiretap may be authorized upon a showing of "probable cause for the belief that the facilities from which, or the place where, the wire, oral or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense"); *see also* United States v. Giordano, 416 U.S. 505, 532–33 (1974) (discussing these subsections).

264 18 U.S.C. § 2518(3)(c); *accord* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 463 (1977); United States v. Kahn, 415 U.S. 143, 153 n.12 (1974).

265 *Kahn*, 415 U.S. at 153 n.12 (citing S. Rep. No. 90-1097, (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112 (Apr. 29, 1968)).

ing agents should be provided only the cell phone numbers from each cell tower dump, as opposed to all the other information typically requested. Then, they can compare the cell phone numbers to determine whether there are any matches at more than one crime scene. If such matches exist, they can then obtain the additional information associated with the matching cell phone numbers.

Second, the wiretap statute dictates that the interceptions of communications "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception."[266] For purposes of applications seeking cell tower dumps, the government should not only seek to minimize the intrusion into the private lives of individuals who are not the subject of the ongoing criminal investigation, but provide an explanation of how it intends to minimize this intrusion. Any application should address what protocol will be employed to deal with the numerous telephone numbers and other information obtained that do not have any role in the purported criminal offense.[267] Such a protocol would include an explanation of methodology in obtaining the telephone numbers as well as an explanation about how non-relevant numbers would be disposed of after the investigation and any subsequent prosecution had concluded.

Third, the individuals whose personal information was swept up in the cell tower dump during the course of the criminal investigation should be notified by either the telecommunications provider or the government after such reasonable time that notification would not jeopardize the ongoing criminal investigation.[268] If an individual's home or other property were searched pursuant to a search warrant, then notice would be required pursuant to Rule 41. Here, notice of the government's access to individuals' personal information should not go unreported to the affected individuals. Surely, some of the 150,000 persons with information compromised in *Capito*, or the 179 persons in *Soto* whose records were investigated and made publicly

---

266 18 U.S.C. § 2518(5); *see also* Scott v. United States, 436 U.S. 128, 139–41 (1978) (discussing minimization of the interception of non-relevant telephone calls).

267 *See In re* Search of Cellular Telephone Towers, Nos. C-13-523M, C-13-525M, C-13-526M, C-13-527M, C-13-528M, 2013 WL 1932881, at *2–3 (S.D. Tex. May 8, 2013).

268 *See* 18 U.S.C. § 2518(8)(d) (providing that persons whose telephone communications are intercepted be notified within 90 days); *see also* United States v. Dalia, 441 U.S. 238, 248 (1979) ("In United States v. Donovan, 429 U.S. 413, 429 n.19 (1977), we held that Title III provided a constitutionally adequate substitute for advance notice by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance.").

available would like to be aware of that situation. This measure would enable persons affected by the investigation who are ultimately not targets of the investigation to ensure that their most personal data are not compromised. They should be told what information of theirs the government obtained and what the government plans to do with it after the criminal investigation and any prosecution is concluded.

The use of these simple measures could ensure that everyone's constitutional rights are properly safeguarded. Moreover, it would provide those whose records were accessed with knowledge as well as the ability to prevent improper or illegal use of their personal information.

CONCLUSION

This Article does not seek to ban the use of cell tower dumps. In certain contexts, cell tower dumps can be extremely useful. For example, in the classic scenario of a team of bank robbers who have a similar method of robbing various banks in an area, a cell tower dump with the proper safeguards can be an effective, and constitutional, law enforcement weapon.[269]

The problem with cell tower dumps is that the federal government typically applies for them pursuant to 18 U.S.C. § 2703. However, this statute does not address cell tower dumps. Additionally, the Fourth Amendment has evolved to provide privacy protections for new electronic surveillance techniques, including cell tower dumps. People have a reasonable expectation of privacy in the cell site location information recorded by cellular providers.

Ultimately, it would be preferable for Congress to enact new legislation specifically addressing cell tower dumps, but that has not yet happened and does not appear likely in the near future. Any new legislation would still have to adhere to constitutional mandates or risk being found unconstitutional. Indeed, even the Fifth Circuit, in alluding to cell tower dumps, has distinguished them from applications for historical cell site information.

Applications for cell tower dumps should seek warrants based on a demonstration of probable cause to obtain the cell site location information. Moreover, law enforcement officials and the courts

269 *See generally* Brian L. Owsley, *Cops and Robbers: The Use of Cell Tower Dumps to Investigate Bank Robberies*, AMER. CRIM. L. REV. (2013), http://www.americancriminallawreview.com/Drupal/blogs/blog-entry/cops-and-robbers-use-cell-tower-dumps-investigate-bank-robberies-01-26-2013.

should address the privacy rights of third-party individuals whose information is obtained through cell tower dumps. Such individuals need to be notified when law enforcement officials obtain their information. There also needs to be a mechanism whereby this private information is no longer in the government's possession once the criminal investigation or prosecution has concluded.

In the end, protocols and probable cause with a warrant will ensure that privacy rights are balanced and protected against law enforcement's interest in using electronic surveillance such as cell tower dumps to further criminal investigations.