Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes

WILLIAM CURTISS*

The recent proliferation of location-based technology and services for cell phones have many wondering if society has forfeited its reasonable expectation of privacy in personal location. Further, the ability of police investigators to accurately track criminal suspects has provided a popular, well-publicized tool to crime fighters. But much of the development of cell phone tracking technology has taken place out of the public view and is only now coming to the surface. As such, the statutory and constitutional framework for analyzing the use of these new technologies has not been significantly modified for years and is entirely incoherent. This Note focuses on one particular tracking technology — triggerfish — to make a practical and Fourth Amendment argument for consistency in police implementation of location tracking, and a defense of personal privacy amidst twenty-first century changes.

* Staff member, COLUM. J.L. & SOC. PROBS., 2010–2011. J.D. Candidate 2012, Columbia Law School. The author would like to thank Steven G. Kalar for suggesting the idea for this note, and all those who have offered invaluable advice and feedback along the way: Professor Daniel C. Richman, Professor Philip M. Genty, Professor James E. Tierney, Tony Curtiss, Marta Osterloh, and Maureen Kellett. The author would also like to give special thanks to the staff and editorial board of the *Journal* for all their hard work.

I. INTRODUCTION

Academic commentators and journalists have paid close attention in recent years to the ability of police investigators to compel telecommunication providers to facilitate real time cell phone tracking with less than a showing of probable cause.[1] This tracking method records a cell phone's periodic communication with cell phone towers in order to hone in on the cell phone's location with varying degrees of accuracy.[2] A heated statutory and constitutional debate has raged between privacy advocates and criminal prosecutors and investigators over the past six years.[3] The debate has centered on what level of prior showing is required before the government can acquire this information: a warrant showing probable cause, or only a lesser demonstration of relevance? So far, legislatures and the Supreme Court have been silent on the issue, and the debate has come to a relative

1. Most published academic articles have been student notes. *See* Patrick T. Chamberlain, Note, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745 (2009); Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421 (2007). Influential legal scholars have commented on the matter mostly through more informal channels such as blogs. *See, e.g.,* Orin Kerr, *Fourth Amendment Stunner: Judge Rules That Cell Site Data Protected by Fourth Amendment Warrant Requirement*, THE VOLOKH CONSPIRACY (Aug. 31, 2010, 2:46 AM), http://volokh.com/2010/08/31/fourth-amendment-stunner-judge-rules-that-cell-site-data-protected-by-fourth-amendment-warrant-requirement/; M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413 (2007). The media and legal organizations such as the American Civil Liberties Union (ACLU) or Electronic Frontier Foundation (EFF) have been most vocal on the issue. *See* Anne Barnard, *Growing Presence in the Courtroom: Cellphone Data as Witness*, N.Y. TIMES, July 6, 2009, at A16; David Kravets, *Court OKs Warrantless Cell-Site Tracking*, WIRED (Sept. 7, 2010, 6:33 PM), http://www.wired.com/threatlevel/2010/09/cell-site-data; *Cell Tracking*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cell-tracking (last visited Sept. 19, 2011) [hereinafter *Cell Tracking*].

2. *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 751 (S.D. Tex. 2005).

3. *See 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. 77–78 (2010) [hereinafter *Subcommittee Hearing*] (statement of U.S. Magistrate Judge Stephen Wm. Smith, Southern District of Texas), *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.PDF.

standstill.[4] To date, the Third Circuit is the only federal appellate court to offer an opinion on the subject.[5]

In the midst of this controversy, however, relatively little attention has been paid to the increasingly common police practice of bypassing the telecommunication companies and acquiring this location data directly through the use of "triggerfish" or "cell site simulators."[6] Triggerfish are portable devices that can be used to track cell phones by mimicking cell phone towers and tricking cell phones into sending their signaling information, which can then be used to track the phone.[7] By allowing police to bypass the phone companies, these devices have the capacity to shift the focus of the legal debate. As triggerfish diminish the necessity of real time cell site orders, the legal battle will move towards access to historical cell site data and judicial oversight of triggerfish use.

This Note examines the unique legal and practical implications of the use of triggerfish. By comparing the technology to the present understanding of cell site location data and current Fourth Amendment legal theories, this Note argues for consistency across the statutory scheme, and for a closer examination of the privacy concerns implicated by increased triggerfish use.

Part II of this Note discusses the statutory and constitutional foundation for cell phone tracking via acquisition of cell site data from telecommunications providers. It directs particular attention towards the precision of cell site tracking, and emphasizes factors commonly overlooked in the debate over the technology's ability to invade the private sphere. The statutory scheme governing traditional cell site tracking does not apply to triggerfish in precisely the same manner, as triggerfish do not require phone

---

4. *Id*.

5. *In re* Application of the United States an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010). This case addressed *historical* cell phone location tracking, however, not real time or prospective tracking. *Id.*

6. Julian Sanchez, *FOIA Docs Show Feds Can Lojack Mobiles Without Telco Help*, ARS TECHNICA (Nov. 16, 2008, 10:45 PM), http://arstechnica.com/tech-policy/news/2008/11/foia-docs-show-feds-can-lojack-mobiles-without-telco-help.ars.

7. U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL 38–40 (2005) [hereinafter SURVEILLANCE MANUAL].

company assistance.[8] But understanding the current state of the location tracking debate is essential in ascertaining the unique privacy concerns invoked by triggerfish, as discussed in Part IV, and how best to construct a comprehensive location surveillance legal framework that aids police investigations and respects the Fourth Amendment.

Part III of this Note examines the latest developments in the debate over location tracking, and the practical and doctrinal aftermath of the first court of appeals decision addressing the issue in September 2010. It posits that real time cell site orders have diminished in value for police investigators, and that the legal argument will focus on historical cell site orders and triggerfish in the future.

Part IV looks at the relatively unexamined triggerfish technology. It parallels the structure of Part II in its discussion of the technology and statutory foundation, and then applies the current Fourth Amendment understanding of cell site data to this direct acquisition of location information, mindful of nuances particular to triggerfish that alter the constitutional analysis. In conclusion, this Note argues that, from a practical as well as Fourth Amendment perspective, triggerfish should be operated consistently with traditional cell site tracking use and should carry a comparable level of privacy protection.

II. CELL SITE LOCATION TRACKING AND LIMITS ON UNFETTERED POLICE ACCESS

The ability of government agents to track the location of individuals is governed by a combination of constitutional and statutory rules. The Fourth Amendment states that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ."[9] The Supreme Court held in the landmark Fourth Amendment case

8. *See* Stored Communications Act (SCA), 18 U.S.C.A. § 2701–2712 (West 2009); Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001–1010 (2006).

9. U.S. CONST. amend. IV. The Fourth Amendment concludes with the directive that warrants be "supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*

Katz v. United States that an individual is protected from warrantless search or seizure if that individual possesses a subjective expectation of privacy, and if society recognizes that expectation as reasonable.[10] Information and activities inside a private home are therefore protected from government intrusion, but objects, activities and statements outside the home in plain view are not protected.[11]

An individual's personal location can reveal information that falls under the purview of the Fourth Amendment, but since people travel frequently in plain view of the public, this is not always the case.[12] As such, the Fourth Amendment does not definitively answer the question of whether government investigators can access tracking information without first making a showing of probable cause to the court.[13] Congress has offered some legislative restrictions on the use of personal location information, such as the federal tracking device statute, but there are few bright line boundaries.[14] Adjudicating the possible limitations on police access to certain tracking technology requires close examination of the particular technology, as well as analysis of how the technology fits into the overlapping constitutional and statutory privacy scheme.

Part II.A of this Note looks at the technology underlying traditional cell site tracking. Parts II.B and II.C then examine the statutory limitations on police access to this location information, and the controversial "hybrid theory" set forth by the government that allows for warrantless tracking via the combined authority of multiple federal statutes. Part II.D then examines the constitutional limits on cell site tracking imposed by the Fourth Amendment. These statutory and constitutional frameworks are essential in understanding how the more recent triggerfish tech-

10. 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

11. *Id.* *Katz* held that conversations inside a public phone booth picked up by a listening device on the outside of the booth were protected by the Fourth Amendment, as the enclosed phone booth was a "temporarily private place" and the phone user had a reasonable expectation of privacy. *Id.* at 351–52, 360–61.

12. *See* United States v. Karo, 468 U.S. 705, 715 (1984).

13. *See infra* Part II.D.

14. *See* 18 U.S.C. § 3117 (2006). *See also* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (addressing the recent debate regarding the installation of GPS tracking devices on automobiles), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (2011).

nology fits into the debate: how triggerfish differ from traditional cell site tracking, how statutory and constitutional limits affect triggerfish specifically, and how, from a practical viewpoint, triggerfish moot much of the argument over real time cell site tracking.

A. CELL SITE TRACKING TECHNOLOGY

Modern cell phones operate by sending out periodic signals or "pings" to nearby cell towers.[15] These signals help determine through which towers to route incoming and outgoing calls in order to ensure the best reception.[16] In addition, location and signal information is conveyed to towers during incoming and outgoing phone calls.[17] These signals can be used to track the location of a cell phone as it travels away from and towards various cell towers.[18] Cell towers in rural areas tend to be as far apart as ten miles, but in urban areas they can be a half-mile apart or closer.[19] In recent years, cellular technology has improved to such an extent that in some locations, cellular towers target specific buildings and even rooms in buildings.[20]

This high density of cell towers can be used to triangulate the location of a cell phone using Time Difference of Arrival (TDOA), Angle of Arrival (AOA), or a combination of both techniques.[21] TDOA measures the relative times at which the signal from a mobile device reaches multiple cell towers.[22] AOA compares the relative angles at which at least two towers receive a cell phone signal.[23] These technologies are publically advertised to be accu-

---

15. Marshall Brain et al., *How Cell Phones Work*, HOW STUFF WORKS, http://electronics.howstuffworks.com/cell-phone1.htm (last visited Sept. 19, 2011).

16. *In re* Application of the United States for an Order Authorizing the Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel., 2009 WL 159187, at *1–3 (S.D.N.Y. Jan. 13, 2009).

17. Brain et al., *supra* note 15.

18. *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005).

19. *In re* Applications of the United States for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 78 (D. Mass. 2007).

20. *Subcommittee Hearing*, *supra* note 3, at 15–16 (statement of Matt Blaze, Associate Professor of computer information science at the University of Pennsylvania).

21. McLauglin, *supra* note 1, at 426.

22. *Track Cellphone Without GPS with U-TDOA*, DHYRA.COM (Dec. 14, 2010, 8:20 PM), http://www.dhyra.com/2010/12/track-cellphone-without-gps-with-u-tdoa.html.

23. *Id.*

rate to within fifty meters, but some sources indicate that precision may be even greater.[24] TruePosition, a company that equips telecommunications providers with triangulation technology, offers a hybrid system that combines TDOA (network-based) and GPS (satellite and handset based) technology for accuracy within fifteen meters.[25]

At the direction of the FCC, telecommunication providers have spent years developing and improving an "Enhanced 911" technology capable of triangulating the location of a cell phone to allow emergency services to quickly arrive with aid.[26] Through this mandate the government has overseen the creation of an infrastructure that can also be particularly useful to law enforcement investigations. Even if the cell site information is only taken from the single nearest tower and not from multiple towers — preventing the exact triangulation of the phone's position — law enforcement agencies with access to this information could still deduce the location of the target cell phone to within a few hundred feet.[27]

It is important to keep in mind the practical utility of this technology when evaluating the legal arguments for various standards. Cell phone tracking is an extremely useful technology for law enforcement, especially with regard to kidnappings and missing persons.[28] In these time-sensitive operations, prosecutors assert that requiring a showing of probable cause could signifi-

---

24. *Subcommittee Hearing*, *supra* note 3, at 95–96 (statement of Matt Blaze). *See also infra* notes 105–107 and accompanying text.

25. TRUEPOSITION, TRUEPOSITION GUIDE TO LOCATION TECHNOLOGIES 5–6 (2009) [hereinafter TRUEPOSITION] (on file with *Columbia Journal of Law & Social Problems*).

26. The FCC mandates that by 2012, Enhanced 911 must be capable of locating 67% of calls to within 100 meters and 95% to within 300 meters. Janice Partyka, Editor's Reply, *How Accurate E911?*, GPS WORLD, Nov. 2007, *available at* http://findarticles.com/p/articles/mi_m0BPW/is_11_18/ai_n27458948/?tag=content;col1. If some form of handset-based technology is used (e.g., GPS), Enhanced 911 must be accurate to within fifty meters for 67% percent of calls and 150 meters for 95% of calls. *Id*.

27. *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 598 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

28. Albert Gidari, Jr., *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535, 544 (2007); *Subcommittee Hearing, supra* note 3, at 57 (testimony of Richard Littlehale, Assistant Special Agent in Charge, Technical Services Unit, Tenn. Bureau of Investigation); Lynne Terry, *Washington Police Used Cell Phone Pings to Zero in on Fugitive in Amber Alert*, OREGONIAN (Mar. 2, 2011, 5:44 PM), http://www.oregonlive.com/pacific-northwest-news/index.ssf/2011/03/washington_police_used_cell_phone_pings_to_zero_in_on_fugitive_in_amber_alert.html.

cantly slow operations.[29] The technology has also been indispensable for investigators tracing the movements of suspected drug traffickers, human smugglers, and, in a few high profile cases, corrupt public officials.[30] In a recent highly publicized murder trial in Philadelphia, investigators were able to overcome the suspects' use of prepaid cell phones, which are generally difficult to track, through improvements in cellular tracking capabilities.[31]

But, of course, privacy concerns are also pronounced in this area, as is the risk of abuse.[32] The government's ability to precisely track a citizen's every move with minimal legal process seems to speak directly to the Orwellian worst-case scenario prophesized by privacy advocates.[33]

---

29. Gidari, *supra* note 28, at 544.

30. William Fisher, *Gov't Sued over Cell Phone Tracking*, INTER PRESS SERVICE (Feb. 22, 2010), http://ipsnews.net/news.asp?idnews=50423; Michael Isikoff, *The Snitch in Your Pocket*, NEWSWEEK (Feb. 18, 2010, 7:00 PM), http://www.newsweek.com/2010/02/18/the-snitch-in-your-pocket.html ("Jack Killorin, who directs a federal task force in Atlanta combating the drug trade, says cell-phone records have helped his agents crack many cases, such as the brutal slaying of a DeKalb County sheriff: agents got the cell-phone records of key suspects — and then showed that they were all within a one-mile area of the murder at the time it occurred, he said. In the fall of 2008, Killorin says, his agents were able to follow a Mexican drug-cartel truck carrying 2,200 kilograms of cocaine by watching in real time as the driver's cell phone 'shook hands' with each cell-phone tower it passed on the highway. 'It's a tremendous investigative tool,' says Killorin. And not that unusual: 'This is pretty workaday stuff for us.'").

31. Investigators in the Chae case were able to combine eyewitness testimony of phones used during the burglary-homicide with sufficiently accurate cell phone location records to demonstrate co-defendants' traveled from their home neighborhood to the neighborhood of the victim. Derrick Nunnally, *Phone Tracking Crucial in Murder Trial*, PHILA. INQUIRER (Jan. 20, 2010), http://articles.philly.com/2010-01-20/news/25210157_1_cell-phones-murder-trial-montgomery-township.

32. *See* Barnard, *supra* note 1 ("[A] sheriff in Alabama told a carrier he needed to track a cell phone in an emergency involving a child — she turned out to be his teenage daughter, who was late returning from a date."). *See also* Isikoff, *supra* note 30 ("A potentially more sinister request came from some Michigan cops who, purportedly concerned about a possible 'riot,' pressed another telecom for information on all the cell phones that were congregating in an area where a labor-union protest was expected."); *Subcommittee Hearing*, *supra* note 3, at 102–03 (testimony of Marc J. Zwillinger).

33. *Cell Tracking*, *supra* note 1 (stating the EFF's goal of "stop[ping] the government from turning the cellular phone system into a vast network for warrantless physical surveillance and . . . ensur[ing] that Big Brother stays out of your pocket").

B. STATUTORY FOUNDATION FOR POLICE ACQUISITION OF CELL SITE LOCATION INFORMATION[34]

Statutory authority for law enforcement to acquire cell site tracking information comes from the ambiguous intermingling of multiple federal statutes: the Pen/Trap Statute and the Stored Communications Act, which are both part of the Electronic Communications Privacy Act, and the Communications Assistance for Law Enforcement Act.[35]

The Pen/Trap Statute,[36] part of the Electronic Communications Privacy Act of 1986 (ECPA), was enacted in response to the landmark 1979 Fourth Amendment case *Smith v. Maryland*, which held that individuals have no reasonable expectation of privacy in the telephone numbers they dial.[37] *Smith v. Maryland* addressed the police use of pen registers, which record numbers dialed out by a target phone, and later was applied to the use of trap and trace devices, which record phone numbers called into a phone.[38] After the Court stripped this dialing information of any Fourth Amendment protection, Congress enacted the Pen/Trap Statute to add some minimal legal barriers to indiscriminate pen/trap use.[39] The statute allows law enforcement to install or use a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which wire or electronic communication is

---

34. The debate over cell site location tracking has centered on the construction of multiple federal statutes and the use of the technology by federal officials. Whether state agents can apply for cell site info without a showing of probable cause depends on the construction of the comparable state statutes. Many state statutory schemes mirror the federal statutes, though. Fourth Amendment limitations to cell phone tracking apply equally to both state and federal agents. *See* Mitchell v. State, 25 So. 3d 632 (Fla. Dist. Ct. App. 2009); John Curran, *ACLU Sues State Over Police Cell Phone Tracking*, BRATTLEBORO REFORMER, Mar. 17, 2010.

35. Commentators, judges and lawmakers have frequently complained that the statutes are impossible to reconcile with each other and "woefully outdated." Tony Romm, *Citing Cell Phone Tapping, Leahy Calls for Privacy Hearings*, THE HILL (Feb. 12, 2010, 4:58 P.M.), http://thehill.com/blogs/hillicon-valley/technology/80953-citing-cell-phone-tapping-case-leahy-calls-for-privacy-hearings.

36. 18 U.S.C. §§ 3121–3127 (2006). The Pen/Trap Statute was subsequently revised in 2001 by the USA PATRIOT Act, which is relevant for the purpose of triggerfish. *See infra* Part IV.B.

37. 442 U.S. 735, 745–46 (1979).

38. *Id.* at 736; 18 U.S.C. § 3123.

39. S. REP. NO. 99-541, at 1–2, 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555–56, 3568 [hereinafter S. Rep. No. 99-541].

transmitted."[40] An application for such a pen register or trap and trace device will be granted if a government attorney certifies that "the information likely to be obtained is relevant to an ongoing criminal investigation."[41] This is an easy burden to meet, as approval of a pen/trap order is a ministerial act for magistrate judges, and courts usually will not look closely at relevance, only at the certification of the government attorney.[42]

The Communications Assistance for Law Enforcement Act of 1994 (CALEA)[43] was enacted a decade after the ECPA to clarify duties of telecommunications companies in cooperating with law enforcement.[44] It specifies that pursuant to a court order, telecommunication providers must enable the government to access call-identifying information "before, during, or immediately after the transmission of a wire or electronic communication."[45] Call-identifying information is defined as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication."[46] However, CALEA provides some privacy protection since, "with regard to information acquired *solely* pursuant to the authority for pen registers and trap and trace devices . . . such call-identifying information shall *not* include any information that may disclose the physical location of the subscriber."[47]

The government, in arguing for access to cell phone tracking with some lesser showing than probable cause, has focused on the Stored Communications Act (SCA)[48] as the added authority that would permit the disclosure of "the physical location of the subscriber."[49] The SCA, a part of the ECPA, states that "[a] governmental entity may require a provider of electronic communication service . . . to disclose a *record* or other information pertaining to a subscriber to or customer of such service" if the governmental

40. 18 U.S.C. § 3127(3).
41. *Id.* § 3122(b)(2).
42. United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995); United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990).
43. 47 U.S.C. §§ 1001–1010 (2006).
44. H.R. REP. NO. 103-827, at 1 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3489 [hereinafter H.R. REP. NO. 103-827].
45. 47 U.S.C. § 1002(a)(2)(A).
46. *Id.* § 1001(2).
47. *Id.* § 1002(a)(2)(B) (emphasis added).
48. 18 U.S.C.A. §§ 2701–2712 (West 2009).
49. 47 U.S.C. § 1002(a)(2)(B).

entity "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[50] Arguing that "record" includes signaling information and cell site data forms the core of the government's "hybrid theory."[51]

Governing both the SCA and the Pen/Trap Statute, as parts of the ECPA, is the ECPA's definition of "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . but does *not* include . . . any communication from a tracking device."[52] A "tracking device" is defined elsewhere in the ECPA by the Mobile Tracking Device Statute as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[53] The use of tracking devices by law enforcement is governed by Rule 41 of the Federal Rules of Criminal Procedure, which requires a warrant and showing of probable cause.[54]

C. THE STATUTORY DEBATE OVER THE GOVERNMENT'S "HYBRID THEORY"

The government has used this statutory scheme to argue that a warrant demonstrating probable cause is not necessary for police to acquire cell site location information. In the government's view, an intermediate standard less than probable cause but greater than ministerial approval suffices. The government's "hybrid theory" combining the Pen/Trap Statute, SCA and CALEA can be summarized as follows. The Pen/Trap Statute allows for the acquisition of "signaling information" with the certification that this information is likely relevant to an ongoing

50. *Id.* § 2703(c), (d) (emphasis added).
51. *See infra* Part II.C.
52. 18 U.S.C. § 2510(12)(C) (2006) (emphasis added).
53. *Id.* § 3117(b).
54. *Id.* § 3117(a). None of these statutes provide for the acquisition of the *contents* of any communication, which would plainly fall under the purview of the Fourth Amendment and be subject to the heightened legal requirements of a Title III wiretap under 18 U.S.C.A. §§ 2510–2522 (West 2010).

criminal investigation.[55] This signaling information includes the "pings" sent between cell phones and cell towers, as well as the signal strength data transmitted during a phone call. However, CALEA states that signaling information that may disclose the physical location of the subscriber cannot be acquired solely pursuant to a Pen/Trap order.[56] The government has interpreted this "solely" to mean that a Pen/Trap order can be combined with some other authority to allow cell site information acquisition. The government maintains that the SCA is such authority.[57] The SCA allows law enforcement to acquire "a record or other information pertaining to a subscriber to or customer of" an electronic communication service upon showing specific and articulable facts that there are reasonable grounds to believe the information sought is relevant to an ongoing criminal investigation.[58] The government argues that this heightened standard of proof, while still less than the probable cause required for a tracking device pursuant to provisions of the ECPA,[59] carries sufficient authority for a magistrate judge to grant an application for prospective cell site data.[60]

Whether the plain language and Congressional intent of multiple, overlapping federal statutes support the so-called "hybrid" authority advocated by the government has brought contentious debate. This is an issue over which "reasonable judges can, and obviously do, disagree," as it hinges on subtle language differences in the Pen/Trap Statute, SCA, and CALEA.[61] The majority of magistrate and district court judges to address the issue in opi-

---

55. 18 U.S.C.A. §§ 3122(b)(2), 3127(3) (West 2009).

56. 47 U.S.C. § 1002(a)(2).

57. 18 U.S.C.A. §§ 2701–2712; *see also In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d 294, 315 (E.D.N.Y. 2005) ("The government, placing more weight on CALEA's use of 'solely' than that single word will bear . . . vigorously contends that an application made under the SCA and the Pen/Trap Statute together accomplishes what separate applications under each statute might not. For ease of reference, I will call this argument the 'hybrid theory.'").

58. *Id.* § 2703(c), (d).

59. 18 U.S.C. § 3117(a) (2006).

60. *See, e.g.*, 396 F. Supp. 2d at 316 ("Although the essence of the [government's] hybrid theory is that two statutes together accomplish what neither can alone, the argument more precisely rests on a complex chain of inferences derived from several different legislative enactments . . . .").

61. *In re* Application of the United States for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices, 632 F. Supp. 2d 202, 211 (E.D.N.Y. 2008).

nions and published orders have rejected the acquisition of cell site information from telecommunication providers without a showing of probable cause under Rule 41 of the Federal Rules of Criminal Procedure.[62] A sizable minority, on the other hand, have agreed with the government's statutory interpretation, limiting orders only to the extent that they might encroach on Fourth Amendment rights.[63] Further, many federal districts continue to grant these "hybrid orders" under seal, so there is little public knowledge of how many orders are granted per year in many jurisdictions.[64]

The legal issue only first became public in 2005 because magistrate judges began to publish opinions, in part out of frustration with the ambiguous statutory overlap and unwillingness to continue granting the sealed ex parte orders simply "because other judges had done so."[65] Several magistrate judges have since gone to the press in hopes of motivating Congress to act to clarify incongruous statutes.[66] So far Congress has been silent, although

62. *See infra* Part II.D.

63. *See infra* Part II.D.

64. In some districts, potentially hundreds of these orders are granted each year, with over 90% of those orders remaining sealed. Further, unlike wiretaps, pen registers and orders for stored communications data do not have reporting requirements, meaning many individuals will never be aware they have been monitored through cell site location tracking. *In re* Sealing & Non-Disclosure of Pen/Trap/2703(D) Orders, 562 F. Supp. 2d 876, 895 (S.D. Tex. 2008).

65. *Subcommittee Hearing*, *supra* note 3, at 81 (testimony of Magistrate Judge Smith). Judges on either side of the debate have expressed frustration with the current statutory scheme and the need for Congressional action. *Two Pen Register*, 632 F. Supp. 2d at 208 ("Moreover, Congress has not provided the kind of guidance as to the correct manner of combining the Pen Register Statute with the SCA that might be expected if Congress intended such a combination."); *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006) ("[N]either the Pen Register Statute nor CALEA mentions [SCA] at all, and they certainly do not provide any direct authorization for the combination of authority the government proposes. While this is somewhat troubling, it is not fatal to the government's application."); *In re* Application of the United States for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 443 (S.D.N.Y. 2005) ("The idea of combining some mechanism with as yet undetermined features of the Pen Register Statute is certainly an unattractive choice. After all, no guidance is provided as to how this 'combination' is to be achieved."); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) ("Absent any sign that Congress has squarely addressed and resolved those concerns in favor of law enforcement, the far more prudent course is to avoid an interpretation which risks a constitutional collision.").

66. Ellen Nakashima, *Judges Urge Standard Cellphone-Tracking Policy*, WASH. POST, Nov. 14, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/11/13/AR2008111303129.html ("This whole area should be the subject of some uniform legisla-

there have been recent subcommittee hearings on the matter.[67] Until Congress or the courts give greater guidance, the availability of warrantless access to cell site information will vary from district to district, and from magistrate judge to magistrate judge.[68] This is a problem. Besides fostering an ad hoc system with costly unpredictability for police, telecommunications companies, and defendants, this variability might lead prosecutors simply to take their applications to the most permissive judges, thereby creating a de facto warrantless standard for the majority of targeted individuals.[69]

There are a few key points of disagreement between judges who grant hybrid orders (the "minority" position) and those who deny hybrid orders (the "majority" position).[70] These key questions of statutory interpretation and legislative intent are summarized below.

1. *Cell Phones, Cell Site Data, and "Electronic Communication"*

The EPCA states that "electronic communication" does *not* include information from a tracking device, which is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[71] The majority of courts interpret the cell phone — in the context of interception of cell site data — as a tracking device. Therefore data from a cell phone cannot be "electronic communication," and cell site information cannot be records concerning an "electronic communication service" pursuant to the SCA.[72] Under this majority position the SCA does not reach cell site information and thus cannot be used in combi-

---

tion that says let's try and coordinate what's going on here, otherwise it becomes ad hoc. That's not the court's role,' said one U.S. magistrate judge.").

67. *See Subcommittee Hearing*, *supra* note 3.

68. Apparently the Central District of California at one point had two separate cell site application forms: one for magistrate judges who required Rule 41 warrants and one for judges who did not. Nakashima, *supra* note 66.

69. Magistrate Judge Stephen Wm. Smith refers to this as "rent-seeking," if not full on "judge-shopping." *Subcommittee Hearing*, *supra* note 3, at 90.

70. *Id.* at 84 ("Surveying the published opinions, it is fair to conclude that the majority held that probable cause is the appropriate standard for government access to prospective cell site information. A minority of published decisions . . . allow access under the lesser 'specific and articulable facts' standard."); *see also infra* Part II.D.

71. 18 U.S.C. § 2510(12) (2006); *id.* § 3117(b).

72. 18 U.S.C.A. § 2703(c) (West 2009).

nation with the Pen/Trap Statute to compel providers to supply tracking information.[73] The minority position works around this by either finding that a cell phone is not a "tracking device," or by interpreting "electronic communication" as having a separate meaning from "electronic communication service."[74]

Both the minority and the majority interpretations of "electronic communication" are problematic. The minority interpretation ignores that Congress evidently intended some kind of separation between electronic communication data and tracking device data in the ECPA, and opens the door to Fourth Amendment privacy challenges.[75] On the other hand, the majority interpretation potentially undercuts the purpose behind the SCA by finding that *all* cell phone records (the "tracking device") are excluded from the records of an "electronic communication service."[76] Judges on both sides of the debate have made direct appeals to Congress for guidance.[77]

2. *"Real Time" Tracking as a Record Pursuant to the SCA*

The majority of courts find that prospective or real time cell site tracking information cannot be a "record" pursuant to Section 2703(c) of the Stored Communications Act because it is not stored information within the purview of the SCA.[78] The minority position holds that cell site information is a record because it is first

---

73. *In re* Application of the United States for an Order Authorizing the Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel., 2009 WL 159187, at *4 (S.D.N.Y. Jan. 13, 2009); *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Service to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 604 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010); *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register Device, a Trap & Trace Device, and for Geographic Location Info., 497 F. Supp. 2d 301, 309–11 (D.P.R. 2007).

74. *See, e.g., In re* Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 445 (S.D.N.Y. 2005).

75. *See In re* Application of the United States for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices, 632 F. Supp. 2d 202, 207–08 (E.D.N.Y. 2008).

76. *Id*.

77. *See In re* Application of the United States for an Order for Prospective Cell Site Location Info on a Certain Cellular Tel., 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006); *In re* Application of the United States for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices, 632 F. Supp. 2d 202, 205–08 (E.D.N.Y. 2008); Nakashima, *supra* note 66.

78. 497 F. Supp. 2d at 309.

recorded by the telecommunications provider and then immediately handed over to law enforcement.[79] This statutory debate can be illuminated by contrasting real time cell phone tracking with the acquisition of historical cell site data. Historical data does not have the same problem as real time data, because it more comfortably fits within the definition of a stored business "record" as defined by the SCA.[80] Further, some courts are more amenable to a reduced standard for historical data because it better follows the legislative purpose of the SCA than does real time data, and does not seem as innately analogous to a classical tracking device as defined by the ECPA.[81]

This distinction was played out in front of the Third Circuit in the first cell site location tracking case to reach a court of appeals.[82] This decision is examined in further detail in Part III.

3. *Congressional Intent*

Courts disagree over the Congressional purpose behind the applicable statutes. By enacting the tracking device statute, did Congress intend for *all* devices capable of tracking movement to be backed by a showing of probable cause pursuant to Rule 41? As seen in the Senate Report of the Tracking Device Statute, the 1986 legislation had in mind the kind of "homing devices" in use at the time, not some future development of tracking technology.[83] The statute contemplated regulation of "devices . . . used by law enforcement personnel to keep track of the physical whereabouts of the sending unit . . . ."[84] In 1986 this sending unit emitted ra-

---

79. 632 F. Supp. 2d at 207.

80. 18 U.S.C.A. § 2703(c).

81. *In re* Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 622 F. Supp. 2d 411, 418 (S.D. Tex. 2007); *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 79–81 (D. Mass. 2007).

82. *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Service to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).

83. S. REP. NO. 99-541, *supra* note 39, at 9. (Describing mobile tracking devices as "one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder. Such 'homing' devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.").

84. *Id.*

dio signals to enable its tracking. Today, this sending unit is more commonly a phone emitting signals to enable cellular communication, but also to enable location information.[85] Since the drafters twenty-five years ago likely did not have cellular telephones in mind, the same question common to most modern Fourth Amendment concerns arises: what is more important, the method of search as defined by the strict statutory language, or the result of the search as reflected in the purpose underlying the statute?[86]

In the context of CALEA, by including "solely" did Congress intend for location tracking to be available through a statute like the SCA (enacted at the same time as the Pen/Trap Statute), which requires less than a showing of probable cause?[87] Legislative history provides little guidance. The House Report states that CALEA "[e]xpressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information, other than that which can be determined from the phone number."[88] There is no mention of any other statute that might provide this authority, including the SCA.[89] CALEA has provisions providing both for increased police access to wiretapping technology, as well as privacy protections for information like financial records and location data.[90] It is therefore unclear whether Congress intended to require warrants for location tracking data, or left the option open for an intermediate standard such as the "hybrid order." Courts tend to agree that the Congressional records do not offer clear answers either way,

85. *See supra* Part II.A.

86. *See* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303 (2002). Simmons' "results of the search versus method of the search" argument is not directly related to this kind of statutory analysis, but the general competing perspectives on the Fourth Amendment are as follows: should we view a technology's Fourth Amendment implications through the lens of how the specific technology works, or through what the technology "seizes" in its use? Do we need to concern ourselves with statutory or blueprint specifics, or should we take a more results-driven approach in ascertaining "reasonable expectations of privacy?" *Id.* at 1303–07.

87. 47 U.S.C. § 1002(a)(2)(B) (2006).

88. H.R. REP. NO. 103-827, *supra* note 44, at 17.

89. *Id*.

90. *Id.* at 9–10.

and most of the debate has centered on a plain language analysis of the word "solely."[91]

These matters of statutory interpretation and legislative intent are subtle and provide no clear answer. Accordingly, as long as "hybrid orders" steer clear of Fourth Amendment issues, some judges will interpret these ambiguous statutes one way, while other judges will interpret it another. No authoritative precedent exists to guide judges either way.

D. FOURTH AMENDMENT PROTECTIONS FOR CELL SITE LOCATION INFORMATION

Since the Supreme Court found in *Smith v. Maryland* that an individual has no reasonable expectation of privacy in the telephone numbers he or she dials, law enforcement need only overcome a low legal hurdle to use a traditional pen register or trap and trace device.[92] When "signaling information" can be used to track an individual, however — instead of merely to gather incoming and outgoing telephone numbers — Fourth Amendment concerns become more pronounced. As applied to the tracking of planted beepers, the Supreme Court held in the 1983 case *United States v. Knotts* that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[93] Just a year later, however, the Court explained in *United States v. Karo* that the monitoring of a beeper in a private residence closed to visual surveillance would violate the Fourth Amendment if not undertaken pursuant to a warrant and a showing of probable cause.[94]

---

91. *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 456–57 (S.D.N.Y. 2006). It is interesting to note that in the entire United States Code, the phrase "solely pursuant" only appears in 47 U.S.C. § 1002(a)(2). *In re* Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 442 (S.D.N.Y. 2005).

92. 442 U.S. 735, 742 (1979).

93. 460 U.S. 276, 281 (1983). In *Knotts*, police followed suspects after they purchased drug ingredients through both visual surveillance and the use of a beeper planted in the purchased chemical containers. *Id.* at 278–79.

94. 468 U.S. 705, 714–15 (1984). *Karo* followed similar facts to *Knotts*, except police in *Karo,* without a warrant and without being able to visually observe its location, used a planted beeper to ascertain that the target container was inside a private warehouse. *Id.* at 714–15. Courts have also determined, in several unpublished opinions, that an individual does not have a legitimate expectation of privacy in items that are not in the indi-

Courts have frequently followed the *Knotts* and *Karo* public/private analysis when reviewing requests for cell site data. As a general rule, the warrantless location-tracking of an individual on public streets is permissible, but as this tracking narrows its range and focuses on movements in the private domain, it implicates Fourth Amendment rights.[95] The problem with cell site location tracking is that this distinction is often difficult to draw, and the courts cannot simply rely on the self-restraint of investigative agencies.[96]

Accordingly, the majority of courts to address the issue have rejected warrantless cell site location tracking.[97] These denials of

---

vidual's name, *i.e.*, where the defendant is not the cell phone's subscriber. United States v. Suarez-Blanca, 2008 WL 4200156, at *67 (N.D. Ga. April 21, 2008); United States v. Skinner, 2007 WL 1556596, at *17 (E.D. Tenn. May 24, 2007).

95. Silverman v. United States, 365 U.S. 505, 511–12 (1961).

96. Katz v. United States, 389 U.S. 347, 356–57 (1967) ("It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. . . . [T]his Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end."). *See also* United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 317 (1972); *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 613 & n.74 ("[R]outine allowance of location information up to the threshold of the private domain would necessitate increasingly-difficult line-drawing at the margins. . . . The Court does not believe that these difficulties can be met by reliance on investigative agencies' self-restraint."), *vacated*, 620 F.3d 304 (3d Cir. 2010).

97. Reported decisions denying warrantless acquisition of multi-tower and triangulation cell site data include: 534 F. Supp. 2d 585; *In re* Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; and (3) Authorizing the Disclosure of Location-Based Servs., No. 07-128, 2007 WL 3342243 (S.D. Tex. Nov. 7, 2007); *In re* Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info., No. 06-MISC-004, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006); *In re* Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, (2) Authorizing the Release of Subscriber & Other Info., (3) Authorizing the Disclosure of Location-Based Servs., Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847 (N.D. Ind. July 5, 2006); *In re* Application of the United States for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134 (D.D.C. 2006); *In re* Application of the United States for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 132 (D.D.C. 2005); *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Nos. [Sealed] & [Sealed] & the Prod. of Real Time Cell Site Info., 402 F. Supp. 2d 597 (D. Md. 2005); *In re* Applications of the United States for Orders Authorizing the Disclosure of Cell Cite Info., Nos. 05-403, 05-404, 05-405, 05-406, 05-407, 05-408, 05-409, 05-410, 05-411, 2005 WL 3658531 (D.D.C. Oct. 26, 2005); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005).

law enforcement agencies' applications have rested largely on statutory grounds, but the possibility of running afoul of the Fourth Amendment has been a key factor in the decisions. As explained by the Maryland district court, "the government cannot guarantee the cell phone and its possessor will remain in a public place. The mere possibility of such an invasion [of privacy] is sufficient to require the prudent prosecutor to seek a Rule 41 search warrant.'"[98]

A minority of courts have granted "hybrid orders" allowing the government to track individuals through cell site information.[99]

Reported decisions denying warrantless acquisition of single tower cell site data during incoming/outgoing calls include: *In re* Application of United States for an Order Authorizing the Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tele., 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009); *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register Device, a Trap & Trace Device, and for Geographic Location Info., 497 F. Supp. 2d 301 (D.P.R. 2007);); *In re* Application for an Order Authorizing the Installation & Use of a Pen Register & Directing the Disclosure of Telecomms. Records for the Cellular Phone Assigned the No. [Sealed], 439 F. Supp. 2d 456 (D. Md. 2006); *In re* Application of the United States for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, 441 F. Supp. 2d 816 (S.D. Tex. 2006); *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., No. 06 Crim. Misc. 01, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006); *In re* Application of the United States for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos. [Sealed] & [Sealed], 416 F. Supp. 2d 390 (D. Md. 2006); *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register &/or Trap & Trace for Mobile Identification No. (585) 111-1111 & the Disclosure of Subscriber & Activity Info. under 18 U.S.C. § 2703, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); *In re* Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d 294 (E.D.N.Y. 2005).

98. 402 F. Supp. 2d at 604 n.10 (quoting *Cell Site Location Auth.*, 396 F. Supp. 2d at 757–58).

99. Reported decisions granting warrantless acquisition of single tower cell site data during incoming/outgoing calls include: *In re* Application of the United States Authorizing the Use of Two Pen Register & Trap & Trace Devices, 632 F. Supp. 2d 202 (E.D.N.Y. 2008); *In re* Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 622 F. Supp. 2d 411 (S.D. Tex. 2007); *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007); *In re* Application for an Order Authorizing the Extension & Use of a Pen Register Device, No. 07-SW-034, 2007 WL 397129 (E.D. Ca. Feb. 1, 2007); *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448 (S.D.N.Y. 2006); *In re* Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 433 F. Supp. 2d 804 (S.D. Tex. 2006); *In re* Application of the United States for an Order: (1) Authorizing the Installation & Use

These courts have also taken notice, however, of these potential Fourth Amendment concerns. They have all specified that the acquired information must be limited to one particular cell phone (not a wide net of numbers) and to that phone's single closest cell phone tower, and that only information related to incoming and outgoing calls can be collected, not the frequent "pings" of which the phone user has no control.[100]

These limitations follow the holding in *Smith v. Maryland* that phone users have no reasonable expectation of privacy in the numbers they voluntarily dial.[101] At the same time, though, they limit the extent to which the phone's "pings" can be used to turn the phone into a constant tracking device, which could implicate both the Fourth Amendment and the federal tracking device statute.[102] Moreover, by negating the capability to triangulate in real time, these limitations attempt to adhere to *Karo* by ensuring the maximum precision of the cell phone tracking be a few hundred feet and not less than fifty feet.[103] Reduced tracking accuracy

---

of a Pen Register & Trap & Trace Device; & (2) Authorizing Release of Subscriber Info and/or Cell Site Info., 411 F. Supp. 2d 678 (W.D. La. 2006); *In re* United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005). No reported decisions have granted warrantless acquisition of multi-tower and triangulation cell site data.

100. 632 F. Supp. 2d at 208 ("Such information, unlike the information revealed by triangulation or by more advanced communications devices like the iPhone, which contain Global Positioning System devices, is not precise enough to enable tracking of a telephone's movements within a home."); 411 F. Supp. 2d at 683 (denying the government access to "(1) any cell site information that might be available when the user's cell phone was turned 'on' but a call was *not* in progress; (2) information that would allow the Government to triangulate multiple tower locations and thereby pinpoint the location of the user; and (3) GPS information on the location of the user, even if that technology is built into the user's cell phone"); *see also* 405 F. Supp. 2d 444.

101. 442 U.S. 735, 742 (1979).

102. 18 U.S.C. § 3117 (2006).

103. Prominent Fourth Amendment academic Orin Kerr, professor at George Washington University School of Law, asserts that applying *Knotts* and *Karo* to cell site data is incorrect under *Smith*. Kerr, *supra* note 1. Kerr argues that location data conveyed by cellular signals is essential to completing cellular phone calls, and as such is analogous to the telephone numbers voluntarily conveyed to telecommunications providers in *Smith*. *Id*. In this view, the Fourth Amendment does not protect cell site data because the user has voluntarily and knowingly forfeited any expectation of privacy by conveying the data to a third party. *Id*. Whether the location tracking penetrates the protected sphere of the private home is irrelevant in Kerr's understanding. *Id.*; *see also* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009). However, the vast majority of courts, if not every court, to address the issue of cell site data, has used this *Knotts*/*Karo* Fourth Amendment framework (including the Third Circuit, the only court of appeals to address the subject). *See, e.g.*, *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 312–

prevents the possibility police could follow a suspect's movements within a private address, as occurred in *Karo*.[104]

While these limitations do help somewhat to alleviate Fourth Amendment concerns, as technology improves many courts still are apprehensive about the possibility of cell phone tracking within the private domain. The government has conceded that in some contexts "cell-site information is actually more precise in locating and tracking a target than a GPS device . . . ."[105] More recently, Congressional hearings and opinions have revealed the extent to which this technology has improved.[106] In his testimony before the Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights and Civil Liberties, Matt Blaze, associate professor of computer information science at the University of Pennsylvania, described how even cell site information strictly limited to a single cell tower can precisely locate an individual:

> So the largest sectors can still be several miles in diameter in rural areas, sparsely populated areas. But the latest technology has trended toward what are called variously microcells, picocells and femtocells that are designed not to serve an area of miles in diameter, but rather to serve a very, very specific location, such as a floor of a building or even an individual room in a building such as a train sta-

---

13 (3d Cir. 2010); *In re* Application of United States for an Order Authorizing the Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tele., 2009 WL 159187, at *5 (S.D.N.Y. Jan. 13, 2009); *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 81 (D. Mass. 2007); *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 462 (S.D.N.Y. 2006); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 752, 756–57 (S.D. Tex. 2005). As such, a complete Fourth Amendment analysis should give credence to both frameworks. For further discussion, see *infra* Part IV.C.

104. Of course, how does the court decide what is too accurate? If a suspect lives on a 500,000 square foot estate, tracking that person's location to within a few hundred feet could covey information about that individual's constitutionally protected movement within the private domain. If a suspect lives in a tiny, one-room apartment, would it be constitutionally permissible to track that individual's location to within 10 feet without acquiring warrant?

105. *In re* Application of the United States for an Order Authorizing (1) the Use of a Pen Register & a Trap & Trace Device with Prospective Cell-Site Info. & (2) the Release of Historical Cell-Site & Subscriber Info., No. 09-104, 2009 WL 1530195, at *2 (E.D.N.Y. Feb. 12, 2009), *rev'd on other grounds*, No. 09-104, 2009 WL 1594003, (E.D.N.Y. Feb. 26, 2009).

106. *See generally Subcommittee Hearing*, *supra* note 3.

> tion, waiting room, or an office complex, or hotel or even a private home. So as we have moved toward very small sector locations, we can, if a user is in one of these very small sectors, essentially determine the [exact] location.[107]

This precision pushes past the boundaries of the Fourth Amendment, as delineated by *Karo*. In locating individuals within rooms of private buildings, the analogy to *Knotts* and surveillance on public streets breaks down.[108] With technological developments in mind, some magistrate judges have decided that the constitutional concerns are too great to permit warrantless tracking, even for historical cell site applications which have been traditionally more favorable to law enforcement.[109]

Beyond the simple *Knotts*/*Karo*, public/private dichotomy, there are several other Fourth Amendment issues that arise with cell phone tracking. Courts have narrowed in on the *Knotts* analogy because it is the cleanest: the rough approximation of location to within a few hundred feet on public land and thoroughfares is equivalent to visible surveillance and does not implicate privacy concerns.[110] But other methods of Fourth Amendment analysis can provide a more nuanced understanding of the cell site tracking debate. These theories include: the Third Party Doctrine and a cell phone user's possible assumption of the risk in voluntarily conveying data to their telecommunications provider;[111] a deeper examination of Reasonable Expectation of Privacy under *Kyllo v.*

---

107. *Id.* at 15–16 (statement of Matt Blaze, Associate Professor of Computer Information Science at the University of Pennsylvania).

108. Tracking individuals as they move between rooms of a public building such as a train station would, of course, not violate the Fourth Amendment. United States v. Knotts, 460 U.S. 276, 281 (1983). But the Fourth Amendment, as expounded by the Supreme Court in *Katz,* does not leave the question of what is permissible or constitutional to the police: "Searches conducted without warrants have been held unlawful notwithstanding facts unquestionably showing probable cause, for the Constitution requires that the deliberate, impartial judgment of a judicial officer be interposed between the citizen and the police." Katz v. United States, 389 U.S. 347, 357 (1967) (internal citations and quotation marks omitted).

109. *In re* Application of the United States for Historical Cell Site Data, 2010 WL 4286365, at *7 (S.D. Tex. Oct. 29, 2010).

110. *In re* Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 622 F. Supp. 2d 411, 418 (S.D. Tex. 2007); *In re* Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 444 (S.D.N.Y. 2005).

111. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

United States and the public's knowledge of this tracking technology;[112] and the recently advanced Mosaic theory under *United States v. Maynard* and the length of surveillance and quantity of data permissible without a warrant.[113] All these areas are important in a discussion of triggerfish technology and are addressed in detail in Part IV.

III. Recent Developments in the Legal Debate over What Standard to Apply to Cell Site Location Information

In 2010, the first and only court of appeals to hear the issue of cell site location tracking published an ambiguous opinion granting limited access to tracking data without a warrant.[114] The approved order was only for historical cell site information, however, and not prospective or real time tracking data.[115] To further muddy the waters, the Third Circuit introduced the idea that, while magistrate judges *could* grant orders for historical data without a showing of probable cause, it is within their discretion to require a warrant if they so choose.[116] This case is noteworthy both as an indication of what the next battles in the cell site debate might be, and as a signal of what is not being addressed: the acquisition of real time data through other means.

The Third Circuit, agreeing with two previous district court decisions granting historical cell site data orders, found that the text and legislative history of the SCA allowed historical location data to be considered a "record" eligible for an intermediate level of privacy protection.[117] The distinction between historical and real time location information weighed heavily into the court's

112. Kyllo v. United States, 533 U.S. 27 (2001).

113. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (2011).

114. *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010).

115. *Id.* at 312.

116. *Id.* at 319.

117. *Id.* at 315. The previous district court opinions were: *In re* Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 622 F. Supp. 2d 411, 418 (S.D. Tex. 2007); *In re* Application of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007).

endorsement of the government's "hybrid" order theory.[118] In the court's understanding, cell site tracking was relatively imprecise, and could not narrow in on movements inside a private residence like more precise GPS tracking.[119] This factual understanding allowed the court to follow previous decisions finding that since the private realm could not be breached by cell site tracking, under a *Knotts*/*Karo* analysis the Fourth Amendment was not implicated.[120] Further, the court held that imprecise *historical* location information is not analogous to a tracking device as defined by statute.[121] The court stated that it could imagine scenarios in which acquiring *real time* cell site data could amount to the use of a tracking device on an individual.[122] As such, the court made sure to emphasize that its decision was limited to historical data, holding that "[i]f [cell site location information] can be used to allow the inference of present, or even future, location, in this respect [it] may resemble a tracking device which provides information as to the actual whereabouts of the subject."[123]

The court tempered its relaxing of privacy protection for historical cell site tracking by holding that it was within the discretion of magistrate judges to grant a hybrid order, or require a Rule 41 warrant.[124] This part of the decision has generated the most discussion, and might become the next major battlefield in the debate, respecting both historical data and real time data.[125] But an equally interesting question raised by the Third Circuit's decision is why has the center of the debate moved to historical cell site data, when, until recently, real time tracking was a more

118. 620 F.3d. at 310–12.
119. *Id.* at 311.
120. *Id.* at 313.
121. *Id.*
122. *Id.* at 312.
123. *Id.*
124. *Id.* at 319.
125. *See* Orin Kerr, *Third Circuit Rules That Magistrate Judges Have Discretion to Reject Non-Warrant Court Order Applications and Require Search Warrants to Obtain Historical Cell-Site Records*, THE VOLOKH CONSPIRACY (Sept. 8, 2010, 2:23 PM), http://volokh.com/2010/09/08/third-circuit-rules-that-magistrate-judges-have-discretion-to-reject-court-order-application-and-require-search-warrants-to-obtain-historical-cell-site-records/. The Third Circuit predominantly based its finding of judicial discretion in the granting of Section 2703(d) orders in the statutory language of the SCA ("may" v. "shall"). 620 F.3d. at 319. Kerr disagrees with this reading, and also thinks that magistrate judges as a matter of law lack any discretion in whether to issue an order if the government satisfies the legal threshold. Kerr, *supra* (citing *Ex Parte* United States, 287 U.S. 241 (1932)).

pressing concern?[126] Magistrate Judges and academic commentators have advocated for years that the Department of Justice appeal warrantless cell site applications that were denied so that appellate courts can adopt a clear decisive standard.[127] It is therefore curious that the first and only hybrid order to reach circuit court review was an order for historical information, when from 2005 until 2008 real time tracking was the main concern and historical tracking was secondary.[128]

While there are mixed reasons for why the government appealed only this single case, the increased law enforcement use of triggerfish devices presents one explanation. The government is likely content to leave the muddled real time cell site case law where it lies: able to acquire hybrid order approval from some judges but not others, while always able to fall back on the use of triggerfish if need be, since triggerfish require far less judicial oversight and process.[129] Historical cell site data is the only information that law enforcement is incapable of acquiring directly, and hence requires the cooperation of telecommunications providers and court orders. This account suggests that, with continued triggerfish use, the real time cell site debate will subside, but the Department of Justice will continue to appeal historical cell site decisions in search of favorable law.

---

126. Real time cell site location tracking burst onto the legal scene in 2005, with many court opinions, academic articles, and news accounts following in the next few years. *In re* Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005); *In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005). Far fewer opinions have focused on historical cell site data, with the first coming in 2007. *In re* Applications of the United States for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007). The first major academic writing about historical cell site tracking came in 2009. Chamberlain, *supra* note 1, at 1753.

127. *Subcommittee Hearing*, *supra* note 2, at 76–77 (testimony of Magistrate Judge Smith).

128. Professor Kerr also argues that the Department of Justice might not even have standing to bring the issue to an appellate court because denials of *ex parte* applications are not appealable final orders. Kerr, *supra* note 1 (citing United States v. Savides, 658 F. Supp. 1399, 1404 (N.D. Ill. 1987)). Kerr appears to be in the minority, however, and the government's standing has been uncontested so far. *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 304 (3d Cir. 2010).

129. *See infra* Part IV.

IV. TRIGGERFISH LOCATION TRACKING DEVICES AND THEIR PLACE IN THE CELL SITE LEGAL FRAMEWORK

A. THE TECHNOLOGY

Triggerfish, also known as cell site simulators or digital analyzers, operate using the same underlying technology as cell site location tracking.[130] The equipment consists of an antenna, an electronic signal processor, and a laptop to analyze the data.[131] Triggerfish imitate cell towers and are able to intercept a target cell phone's cell site data: its telephone number (mobile identification number or "MIN"), its electronic serial number ("ESN"), and the channel or codes identifying the cell location and geographical sub-sector from which the phone is transmitting.[132] This information is conveyed approximately every seven seconds by the phone's registration "pings" whenever the phone is turned on.[133] In addition, this cell site data is conveyed whenever the phone initiates or receives a call, and throughout the duration of the call.[134] The Department of Justice's *Electronic Surveillance Manual* states that a triggerfish "forces" a target cell phone to register this information when the phone is turned on, which suggests that authorities do not simply acquire this information passively while the cell phone user operates her phone.[135]

With this cell site data, triggerfish can track the location of the cell phone in a manner equivalent to tracking by cell towers. The devices register the signal strength and direction of the intercepted frequencies (on a 360 degree display).[136] The agent operating the mobile device can then follow the cell phone signal as

130. The etymology of the name "triggerfish" is unclear, but has become the most common name for the device. "Triggerfish" also refers to a group of about 30 species of tropical fish, named for a trigger mechanism in their dorsal fins that allows the fish to lock themselves tightly into protective crevices. *Triggerfish*, ENCYC. BRITANNICA, http://www.britannica.com/EBchecked/topic/605191/triggerfish (last visited Sept. 21, 2011).

131. SURVEILLANCE MANUAL, *supra* note 7, at 40–41.

132. *Id.*

133. McLaughlin, *supra* note 1, at 426.

134. *Id.*

135. SURVEILLANCE MANUAL, *supra* note 7, at Ch. 38–40.

136. U.S. MARSHALS SERV., TECHNICAL OPERATIONS GRP., POLICY DIRECTIVES (2010) [hereinafter USMS DIRECTIVES].

it travels.[137] Further, by shifting the location of the triggerfish, precise triangulation of the phone's location is possible.[138] This is accomplished by Time Difference of Arrival (TDOA) and Angle of Arrival (AOA) analysis.[139]

The precision of these devices is relatively uncertain, and the heavy redactions in documents the United States Marshals Service produced to the ACLU suggests that the government intends to keep the exact accuracy tightly guarded.[140] There is reason to believe, however, that these devices have improved greatly in precision over the last few years. In the past, law enforcement agencies had to begin their search for a suspect cell phone through cell site location tracking, only later utilizing the triggerfish to focus in on the subject.[141] More and more frequently, agencies are forgoing the heightened legal showing required in cell site location requests and are instead relying on their triggerfish, which now can be useful over a far wider area.[142] Accordingly, the accuracy of triggerfish is approximately comparable to or possibly better than that of cell site tracking (200 to 15 meters).[143]

The usefulness of triggerfish to law enforcement agents is not only limited to location tracking. Unlike the process of acquiring cell site data from telecommunications providers, which requires advanced knowledge of the cell phone number ("MIN") of the intended target, triggerfish can be used to discover a suspect's phone number.[144] Additionally, triggerfish are capable of intercepting the contents of cellular communications, as well as turning the target cell phone into a listening device.[145] In effect, the triggerfish is a sort of mobile, all-in-one electronic surveillance

137. *Id.*
138. SURVEILLANCE MANUAL, *supra* note 7, at 41–48.
139. Chamberlain, *supra* note 1, at 1753.
140. The only redacted sections of the electronic surveillance manual were those dealing with triggerfish and counter-surveillance procedures. USMS DIRECTIVES. The Marshals Service released this information in response to the ACLU's Freedom of Information Act request. Letter from William G. Stewart II, Assistant Dir., Freedom of Info./Privacy Act Staff, Exec. Office for U.S. Attorneys, U.S. Dep't of Justice, to Catherine Crump, Staff Attorney, Am. Civil Liberties Union (Aug. 12, 2008), *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf.
141. Rachel Myers, *With Technology Like This, Who Needs the Law?*, DAILY KOS (Nov. 14, 2008, 8:51 AM), http://www.dailykos.com/story/2008/11/14/104215/56/181/660871.
142. Sanchez, *supra* note 6.
143. TRUEPOSITION, *supra* note 25.
144. SURVEILLANCE MANUAL, *supra* note 7, at 3–16.
145. *Id.* at 41–48.

device. It can determine a target's cell phone number, acquire incoming/outgoing call information in a manner similar to a pen register/trap and trace device, facilitate real time location tracking of varying accuracy[146] without the need to involve a telecommunications provider, and intercept communication content in the manner of a wiretap.[147] Triggerfish can fulfill every function but the acquisition of historical cell site location information.[148]

B. STATUTORY FOUNDATION FOR POLICE USE OF TRIGGERFISH TECHNOLOGY

Before the USA PATRIOT Act revised the Pen/Trap Statute in 2001 to include "signaling information" in its definition of a pen register and trap and trace device, law enforcement agencies used triggerfish without going through any legal process whatsoever.[149] As read through the lens of the House Report, the 2001 amendments made explicit that pen/trap devices could be utilized to "obtain *any* non-content information — 'dialing, routing, addressing, and signaling information' — utilized in the processing and transmitting of wire and electronic communications."[150] This signaling information apparently also includes "packets that merely request a telnet connection in the Internet context," which the Department of Justice construes as permitting the collection of the registration "pings" of cell phones.[151]

Since 2001, a Pen/Trap order certifying that the information sought is likely to be relevant to an ongoing criminal investigation has been required before officers are allowed to use trigger-

146. Accuracy varies depending on whether cell site data acquisition is limited to call information or includes all registration "pings" automatically sent by the phone. *See In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 598 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

147. The content of communications clearly implicates the Fourth Amendment, and law enforcement is sure to disable this feature without a wiretap warrant. 18 U.S.C.A. §§ 2510–2522 (West 2010).

148. This fact adds fuel to the argument that the Department of Justice is pursuing appeals of historical cell site orders but not real time cell site for tactical reasons, namely that only historical cell site orders convey information the government cannot otherwise obtain.

149. 18 U.S.C. § 3122 (2006); *In re* United States for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 199 (C.D. Cal. 1995).

150. H.R. REP. 107-236, at 60 (2001).

151. *Id.*; SURVEILLANCE MANUAL, *supra* note 7, at 41–48.

fish.[152] Because law enforcement agencies can acquire this information without having to order the cooperation of a telecommunications provider, the SCA and CALEA do not apply to triggerfish.[153] Although the argument could be made, no opinion to date has defined a triggerfish device as a tracking device, so probable cause pursuant to the federal tracking device statute is not required either.[154]

C. FOURTH AMENDMENT PROTECTIONS

The Fourth Amendment provides the only real oversight of police use of triggerfish beyond the Pen/Trap Statute. Triggerfish devices are capable of intercepting the content of cell phones, which would unquestionably require a showing of probable cause and a wiretap authorization.[155] As such, law enforcement must disable this feature of triggerfish before using its tracking features.[156] While this capability raises concerns about officer restraint, no court has yet addressed this issue.[157]

But the legal status of unauthorized wiretapping is settled, and hence is less worrisome, than the use of triggerfish for more recent technological capabilities like location tracking. The disincentives for warrantless eavesdropping include suppression of evidence and possible criminal penalties.[158] In contrast, there are no statutory suppression remedies for evidence acquired through

---

152. SURVEILLANCE MANUAL, *supra* note 7, at 41–48.

153. *Id.*; 18 U.S.C.A. § 2703 (West 2009); 47 U.S.C. § 1001 (2006).

154. 18 U.S.C. § 3117. Section 3117 discusses the "installation" of a tracking device. Nothing about the use of a triggerfish requires installation, and the government has successfully suggested that the plain language of the statute does not apply to this type of cell phone tracking. SURVEILLANCE MANUAL, *supra* note 7, at 44–48.

155. 18 U.S.C. § 2518(1)(d) ("Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include . . . a particular description of facts establishing probable cause . . . ."); Katz v. United States, 389 U.S. 347 (1967).

156. SURVEILLANCE MANUAL, *supra* note 7, at 40–41.

157. Courts have worried about officer restraint in the context of cell site data, but as with all discussion of triggerfish, legal commentary has been limited. *See In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Service to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 598 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010) (citing United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 317 (1972)).

158. 18 U.S.C.A. §§ 2511, 2515.

unauthorized use of tracking devices, nor are there clear criminal penalties.[159] Suppression would require the showing of a constitutional violation, and the unsettled debate over cellular location data's place in the *Knotts*/*Karo* distinction shows the difficulty of making that demonstration. Accordingly, the disincentives for extralegal tracking device use are neither explicit nor strong.[160]

Several aspects of the rapid technological improvement of triggerfish location tracking are quite disconcerting from a Fourth Amendment perspective. This Part analyzes these concerns from the perspective of various Fourth Amendment frameworks; the analysis demonstrates that triggerfish carry privacy concerns even more pronounced than traditional cell site data acquisition, and that additional judicial oversight beyond that of a Pen/Trap order should be required before their use is authorized.

1. *Third Party Doctrine*

Some commentators have proposed that the third party doctrine makes the customary *Knotts*/*Karo* examination of cell phone tracking irrelevant.[161] The third party doctrine in Fourth Amendment jurisprudence stands for the proposition that an individual no longer has an expectation of privacy in items that are voluntarily turned over to third parties.[162] The doctrine finds its

159. United States v. Forest, 355 F.3d 942, 949–50 (6th Cir. 2004), *vacated on other grounds sub nom.* Garner v. United States, 543 U.S. 1100 (2005); United States v. Gbemisola, 225 F.3d 753, 758 (D.C. Cir. 2000). Suppression of evidence is not a statutory remedy for violations of the EPCA, which includes the SCA, Pen/Trap Statute and Mobile Tracking Device Statute. *Gbemisola*, 225 F.3d at 758; *see supra* Part II.B. And while the SCA and Pen/Trap Statutes provide for explicit criminal and civil penalties, no such penalties exist for the Mobile Tracking Device Statute. 18 U.S.C.A. §§ 2701, 2702, 2712; 18 U.S.C. § 3121; 18 U.S.C. § 3117. This all leads to a perverse set of incentives for police officers. Wiretapping is clearly protected by evidentiary suppression and criminal penalties, and phone numbers and stored phone records carry with them possible criminal and civil penalties if the proper orders are not acquired. *See supra* note 158 and accompanying text. Tracking devices, however, which presumably require warrants under 18 U.S.C. § 3117 (2006), carry no penalty for improper acquisition (neither suppression nor sanction). 18 U.S.C. § 3117. This provides yet another example of how location information occupies a hazy middle ground in the electronic privacy spectrum, illustrating the need for statutory reform to better guide police investigations.

160. *See supra* Part II.D.

161. Kerr, *supra* note 1.

162. Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 355 (2009).

strongest expression in *Smith v. Maryland*, where the Supreme Court held that an individual retains no expectation of privacy in digits voluntarily conveyed to the phone company to initiate a phone call,[163] and in *United States v. Miller*, where the Court held that financial checks turned over to a bank no longer carried an expectation of privacy.[164] The doctrine can be described as an "assumption of the risk" theory: if an individual conveys private information to a third party, he or she has assumed the risk that the third party may convey the information to the government.[165]

If the third party theory is accepted in the context of cell site location tracking, whether the technology is precise enough to follow an individual in a private residence becomes immaterial.[166] That individual retains no privacy expectation because, by using a cell phone, that individual has turned over the location data inherent to the cell phone's signaling information.[167] For third party doctrine advocates, the *Knotts/Karo* analysis is unnecessary.[168]

However, the third party doctrine, by definition, would not apply in the same fashion to triggerfish use. First, while cell phones tracked by triggerfish are indeed conveying information to third party cell phone companies, that is not the information that the triggerfish device collects. Triggerfish directly acquire data from the cell phone, circumventing the telecommunications provider altogether.[169] Drawing an analogy to *Miller*, police are not acquiring financial information from a third party bank, but are searching the target directly and seizing the bank statement held with a reasonable expectation of privacy.[170] There is simply no third party involved.

---

163. 442 U.S. 735, 742 (1979).

164. 425 U.S. 435, 442–43 (1976).

165. *Id.* The third party doctrine is a fairly complicated and contentious issue. This Note examines it no deeper than necessary for studying triggerfish technology. *See generally* Kerr, *supra* note 103.

166. Kerr, *supra* note 1.

167. *Id.*

168. Though, the *Knotts/Karo* evaluation is relevant for tracking technology that doesn't involve the target individual voluntarily conveying information, i.e. if a GPS chip were implanted in the subject.

169. SURVEILLANCE MANUAL, *supra* note 7, at Ch. 38–40.

170. Orin Kerr, *Fourth Amendment Rights in Online Financial Accounts*, THE VOLOKH CONSPIRACY (Aug. 17, 2009, 12:21 PM), http://volokh.com/2009/08/17/fourth-amendment-rights-in-online-financial-accounts/ ("If the bank sends you your bank statement in the mail, and you open the mail and put the statement on your desk at home, those financial

Second, there is convincing evidence that police investigators use triggerfish in a far more proactive manner than they do cell site tracking. Multiple agency manuals speak of triggerfish "forcing" a target cell phone to register and tricking the phone to believe the triggerfish device is a cell phone tower.[171] As such, the devices are acquiring previously unknown phone numbers instead of collecting data on known numbers as in the context of cell site tracking. More importantly, triggerfish are forcing cell phone users to turn over data, not merely passively collecting data, when it is turned over to a third party via pings or call information originated from the target phone.

The Sixth Circuit's opinion in *United States v. Forest* is important in this regard.[172] While finding no Fourth Amendment protection on the narrower *Knotts*/*Karo* understanding of surveillance on public roads, the court rejected a third party doctrine argument due to the manner in which police in the case acquired the subject cell site data.[173] Officers in *Forest* forced the target cell phone to convey cell site data by repeatedly calling the phone.[174] The court did not approve of this active tracking without a warrant and rejected the notion that cell site data always lacked an expectation of privacy due to its conveyance to a phone company.[175]

Under this *Forest* analysis, triggerfish are an even more egregious means of forced conveyance of private information. If a triggerfish device is used to force a cell phone to register, that information should not lose its Fourth Amendment protection because there was no assumption of the risk on the part of the user. As such, the third party doctrine is generally not applicable

---

records are just as protected by the Fourth Amendment as everything else in your home. What matters is that the home is protected, not that the records would not have been protected if the government had asked for them from the bank.").

171. SURVEILLANCE MANUAL, *supra* note 7, at 38–40.

172. United States v. Forest, 355 F.3d 942 (6th Cir. 2004), *vacated on other grounds sub nom.* Garner v. United States, 543 U.S. 1100 (2005).

173. *Forest*, 355 F.3d at 951.

174. *Id.* at 947.

175. *Id.* at 951–52. *See also In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Service to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 598, 614–15 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

to triggerfish devices, and a narrower examination of reasonable expectation of privacy must be undertaken.[176]

2. *Reasonable Expectation of Privacy*

Since the Supreme Court's landmark decision *Katz v. United States*, the reasonable expectation of privacy test has been the central inquiry into Fourth Amendment questions.[177] The test posits that an individual enjoys Fourth Amendment privacy protection if the individual had a subjective expectation of privacy in a location or situation, and if society recognizes that expectation as objectively reasonable.[178] An important gloss was placed on this test in 2001 by the Supreme Court's ruling in *Kyllo,* which is especially relevant to the police use of triggerfish devices.[179] *Kyllo* held that warrantless monitoring of a house with thermal imaging, which allowed officials to examine the relative temperatures of different rooms in hopes of discovering a marijuana growing operation, violated the Fourth Amendment.[180] In its reasonable expectation of privacy analysis, the Court found importance in the fact that the device was not in general public use.[181] This aspect of the inquiry speaks to society's objective understanding of what is reasonable.

Some scholars have criticized this method of Fourth Amendment analysis, claiming that it penalizes new and unique technology, and patronizes the general public's intelligence and knowledge.[182] In spite of these concerns, this manner of reasonable expectation of privacy analysis remains good law.[183] And triggerfish, compared to other technology, certainly is not in general

176. The Justice Department's *Electronic Surveillance Manual* has a section which differs from the majority view, stating that, like cell site location tracking, only call initiation information can be recorded without a warrant, not the "pings" emitted every few seconds. SURVEILLANCE MANUAL, *supra* note 7, at 40–41. If this is the case, this "forcing" to register concern would be dampened. But the third party doctrine would still appear not to apply because the cell site data is not being acquired from a third party.

177. 389 U.S. 347 (1967).

178. *Id.* at 361 (Harlan, J., concurring).

179. Kyllo v. United States, 533 U.S. 27 (2001).

180. *Id.* at 40.

181. *Id.*

182. Orin Kerr, *Cell Phones, Magic Boxes and the Fourth Amendment*, THE VOLOKH CONSPIRACY (Nov. 8, 2010, 6:05 PM), http://volokh.com/2010/11/08/cell-phones-magic-boxes-and-the-fourth-amendment/.

183. *See supra* notes 177–181 and accompanying text.

public use and is foreign to society's reasonable expectations. Since the proliferation of location-based technology and smart phones, it has been argued that the average consumer knows how a cell phone works and that the cell phone innately conveys location data.[184] But the details of triggerfish have been tightly guarded, and the media and general public alike are largely ignorant of the technology.[185] What is more, triggerfish devices go a step beyond simple cell site location tracking. The cell phone user is not conveying location data to the phone company to enable convenient location services, in this context.[186] The location signaling information is being directly acquired by officers in the field who also have the capability to discover cell phone numbers, force the cell phone to send personal data, and widen the net of the search by incorporating large numbers of cell phones.[187] The general public simply does not know the extent of these capabilities, or of law enforcement's access to them.

3. Knotts *and* Karo

The *Knotts/Karo* inquiry into whether the private sphere was penetrated by the search still remains the most pertinent Fourth Amendment model for cell phone tracking. The debate for both cell site tracking and triggerfish tracking will continue to center on the accuracy of these modes of surveillance.[188] For triggerfish devices, though the information is limited, is seems clear that this technology has improved rapidly over the last few years and is peering into the private realm through its precision.[189] This conclusion comes from testimony about the shrinking size of mi-

184. Kerr, *supra* note 182. *See also* Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, at A1.

185. USMS DIRECTIVES (redacted section on triggerfish); Myers, *supra* note 141.

186. The specific data acquired by a triggerfish is not "reasonably expected to be accessed by the provider's employees in the ordinary course of its business (*i.e.*, for purposes of the provision of services)." *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Service to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 615 (W.D. Pa. 2008) (citing Warshak v. United States, 490 F.3d 455, 469–76 (6th Cir. 2007), *vacated*, 620 F.3d 304 (3d Cir. 2010)).

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

188. See *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).

189. *See supra* Part IV.A.

crocells, picocells and femtocells, from information gleaned by the media, and from changing practices of law enforcement to embrace the ease and precision of triggerfish over the deadlocked debate on traditional cell site protection.[190]

Beyond accuracy, though, triggerfish devices are fundamentally dissimilar to the beeper tracking in *Knotts* or the thermal imaging of *Kyllo*.[191] Although the agent still remains in the field to monitor his or her subject, the utility of triggerfish surpasses the single-functionality of earlier devices. With a triggerfish device, police can find the cell phone number of their target and then force that number to register its location information.[192] This is a far cry from the mere passive following of a subject on public streets. With this forced registration capability, investigators can find and follow an individual, not just follow the suspect once found. The analogy to visual surveillance on a public street is broken, especially considering the high accuracy of these devices.

As this analysis shows, the Fourth Amendment analysis of triggerfish devices is often more difficult than that of traditional cell site data (which was not itself that clean to begin with).[193] The sensitive privacy issues involved in this developing area of triggerfish use suggest that a ministerial Pen/Trap order cannot sufficiently assess the legality of police access. Because triggerfish use generates more Fourth Amendment concerns than traditional cell site tracking, triggerfish devices should ideally operate under greater legal scrutiny, not far less scrutiny as is currently

190. *Subcommittee Hearing*, *supra* note 3, at 15–16 (statement of Matt Blaze); SURVEILLANCE MANUAL, *supra* note 7, at 40–41; Barnard, *supra* note 1, at A16 (noting that it is now "possible to pinpoint a user's position with much greater precision, down to a few dozen yards"); Sanchez, *supra* note 6.

191. Much of the discussion of *Kyllo* centered on whether the thermal imaging penetrated the wall of the private home, and thus was analogous to the Fourth Amendment violation in *Karo*. Kyllo v. United States, 533 U.S. 27, 38 (2001).

192. *See supra* Part IV.A.

193. A fourth privacy framework, as introduced by *United States v. Maynard*, is not as persuasive in this context, but could become so as triggerfish use is further increased. *See* 615 F.3d 544 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (2011). The D.C. Circuit Court held that the continued, month-long tracking of a subject on public streets by GPS compiled such a large quantity of data that it constituted a search. *Id.* As triggerfish devices still require officers to operate in the field, the extent to which this wide scale accumulation of data is possible is uncertain. But it is an interesting area to watch in the coming years.

the case.[194] Triggerfish necessitate greater scrutiny by the magistrate judge, and possibly greater leeway for the judge through judicial discretion within the understanding of the Third Circuit.[195]

V. CONCLUSION

Because triggerfish acquire the exact same information as cell site location tracking, and in many ways do it better and more conveniently, triggerfish use should carry at least as much privacy protection as cell site tracking. Applying various Fourth Amendment exceptions and frameworks to triggerfish supports this proposition, since the arguments for denying protection to traditional cell site tracking simply do not apply to triggerfish. The *Kyllo* notion that reasonableness depends on the result of the search and not the search's method suggests that triggerfish use should require greater judicial oversight and procedure than a mere ministerial Pen/Trap order. The intermediate standard of the SCA explicitly does not apply to triggerfish, however, as triggerfish do not acquire stored records from telecommunications providers. As such, in the absence of legislative input in this area, Fourth Amendment doctrine and the need for consistency across the location tracking statutory scheme require that the government show probable cause before this powerful technology is unleashed.

194. A Pen/Trap ministerial order is significantly less onerous than the hybrid order allowed for cell site tracking, to say nothing of the probable cause warrant standard. United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995); United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990).

195. *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).