1-1-2007

The Fourth Amendment and Cell Phone Location Tracking: Where Are We

Kevin McLaughlin

Follow this and additional works at: https://repository.uchastings.edu/hastings_comm_ent_law_journal

Part of the Communications Law Commons, Entertainment, Arts, and Sports Law Commons, and the Intellectual Property Law Commons

Recommended Citation

Kevin McLaughlin, The Fourth Amendment and Cell Phone Location Tracking: Where Are We, 29 HASTINGS COMM. & ENT. L.J. 421 (2007).

Available at: https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol29/iss3/4
The Fourth Amendment and Cell Phone Location Tracking: Where Are We?

by

KEVIN MCLAUGHLIN*

I. Introduction.................................................................................................................423
II. Background ..................................................................................................................426
   A. How the Technology Works. ..................................................................................426
   B. The Current State of Statutory Protection............................................................428
   C. Fourth Amendment Precedent.............................................................................429
III. Applying the Fourth Amendment to Cell Phone Location Tracking......431
   A. Historical Data Versus “Real-time” Data..............................................................431
   B. Passive Versus Call-based Location Tracking......................................................434
   C. The Level of Specificity of Location Data Gathered..........................................436
   D. Tracking the Suspect at Home. ..............................................................................437
   E. Focus on the Phone Versus the Suspect ...............................................................438
IV. Cell Phone Location Tracking is an Unreasonable Search........................439
   A. Assumption of the Risk is Limited..........................................................439
   B. Property Precepts Remain Prominent.........................................................441
   C. Reasonable Expectations Have Subtly Shifted.............................................442
V. Conclusion ..................................................................................................................444

I. Introduction

Cellular phones are a technological tidal wave. Today there are over 195 million cellular phone subscribers in the United States,1 double the number of subscribers just five years ago.2 Cell phones are increasingly ubiquitous in our society, altering how we communicate and how we interact as a society.3

* University of California, Hastings College of the Law, Juris Doctor Candidate, 2007; B.A., University of California, San Diego. I am indebted to Professor Rory Little, Kevin Bankston and Lee Tien for their insights. All errors and omissions are mine alone.

2. Id.

421
Perhaps the most distinguishing feature of cell phones is that they make us all readily available, no matter where we are. Cell phones come with us everywhere we go: streets, homes, offices, and even those intimate public spaces where a phone ring means embarrassment, such as theaters, high-end restaurants, and even churches.4

But while cell phones follow us everywhere we go, they also allow us to be followed everywhere we go. Cell phones constantly relay their location to the cellular towers that serve their network, providing the cellular service provider with an often quite accurate picture of the location of the phone.5

Such accurate location tracking seems to be a boon for public safety, enabling location tracking of 911 calls made from cellular phones.6 Marketers also stand to benefit through location-based services and advertising.7 Businesses are using this technology to track the whereabouts of mobile employees,8 and states are contemplating using this technology to track traffic patterns.9 One may even track a loved one or "buddy" using this technology.10

The ability to track others has not gone unnoticed by law enforcement. Within the last two years, fifteen published decisions have issued from federal district courts regarding law enforcement applications for cell phone location tracking information. In eleven of these decisions, the court found that probable cause must be shown to obtain cell phone location tracking information and because less than probable cause was shown by law enforcement the requests were

5. See infra Part II A.
10. Moon Ihlwan, Working Late Won't Work Anymore; New Services Can Track You - Or Your Loved Ones - By Cell Phone, BUSINESS WEEK, Oct. 31, 2005, at 40. See also loopt, a start-up that uses GPS and other location technology to enable "social mapping" of others' locations via cellular phone. This technology is currently used by Boost Mobile, a Sprint Nextel Corp. subsidiary claiming over 3.1 million subscribers.
denied. In the other four decisions, surveillance authorization was granted; however, the information sought was arguably more limited


than in most other district court decisions. As more courts face applications for orders granting access to cell phone location tracking, there is little doubt that more published decisions are on the way. In fact, many unpublished orders have already been granted. 13

In light of ever-increasing mobile technology, there is a strong need for Fourth Amendment guidance in this area. As many commentators have noted, dispersed privacy interests of the populace often receive limited attention from legislators compared with the organized interests of law enforcement. 15 Conflicting district court opinions seem headed for appeal, 16 and appellate court decisions can often help spur legislative action. 17 It would not be premature for the Supreme Court to address such a widespread issue. 18

The modern Fourth Amendment test to determine whether an unreasonable search has taken place comes from Justice Harlan's concurrence in Katz v. United States: whether the individual being searched harbored actual expectations of privacy that society is prepared to recognize as reasonable. 19 While this test is broadly applicable, it has been criticized as being “circular” 20 and “self-indulgent.” 21 The Katz test has also had the effect of focusing Fourth Amendment scrutiny on the conduct of the individual, and not on the

13. See S.D. Tex. 1 Decision, 396 F. Supp. 2d at 749 n.2 (noting that in that division, 313 pen register applications were processed in 2004).

http://www.pewinternet.org/pdfs/pip_apr2004_data_memo.pdf. (17% of Internet users have logged on using a wireless device).


16. To date, the government has not pursued appeal of any denials of requests for authorization, although the government did renew an application rejected by Magistrate Judge Peck before District Judge Kaplan. S.D.N.Y. II Decision, 460 F. Supp. 2d 448, 454 (2006).


20. Kyllo, 533 U.S. at 34.

government. Yet despite this widespread criticism, the "reasonable expectation" test remains the modern test of whether a search is reasonable. But as cell phone location tracking illustrates, new technologies have the ability to squeeze our reasonable expectations wafer-thin. Indeed, under the reasonable expectation test, if most Americans were aware that their location could be tracked via their cell phone, all cell phone users would likely forfeit any expectation of privacy in their movements, in return for the technological convenience of the cell phone. Yet it is hard to imagine such a holding sitting well with cell phone users.

Part II of this note will describe how cell phone location tracking technology works, discuss the relevant statutes that regulate such surveillance, and analyze applicable Supreme Court precedent. Part III of this note will show that, depending on a number of factors, cell phone location tracking may or may not qualify as a reasonable search under Katz and its progeny. Part IV of this note argues that because cell phone location tracking implicates a number of core Fourth Amendment doctrines, it should constitute an unreasonable search.

25. Noted criminal defense attorney Milton Hirsch suggests jettisoning the Katz test. Milton Hirsch, Should the Katz Test for Fourth Amendment Interest be Abandoned?, Fourth Amendment Forum, CHAMPION MAGAZINE, November 2003, at 36. Professor Peter Swire claims that Katz is dead. Swire, supra note 15. For a large set of of other critics, including such leading lights as Wayne LaFave, Yale Kamisar, Scott Sundby and others, see George C. Thomas, Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment, 80 NOTRE DAME L. REV. 1451, 1500 (2005).
II. Background

A. How the Technology Works.

Cell phones constantly relay their locations to cellular towers, in order that the next inbound call should be received without a hitch. This process, called "registration," occurs roughly every seven seconds when the cell phone is turned on; the user of the phone does not need to take any action, and is probably unaware that the phone is sending these signals. The only way to stop these signals is to turn the phone off. These location signals are sent on one band—the other two frequency bands that the phone uses are for sending and receiving voice and data.

A mobile telephone switching office (MTSO) manages the cellular system. When a call is received, the MTSO gets the call and then locates the user based on the nearest tower that the user's phone registered with. The call is then sent to the phone by the nearest tower. A similar process works in reverse when the user places a call.

As a user's location moves, the strength of the signal within the cell served by that tower may diminish. Meanwhile, as the user gets closer to a second tower, that tower will recognize the increasing strength in signal. The towers measure the strength of signal—and thus the relative location of the cell phone—through Time Difference of Arrival (TDOA) or Angle of Arrival (AOA) methods. TDOA calculates the amount of time it takes a signal to travel from the phone to the tower in order to calculate the approximate location of the phone. AOA calculates the approximate location of the phone by measuring the angle at which the tower receives the phone's signal. Based on these measurements, the MTSO will then send a signal to the cell phone's control channel that it is time to switch to the frequency of the nearer tower, and the phone will continue the call uninterrupted despite changing towers.

A very general sense of a phone's is can be gathered by tracking the location of the tower being used during a call. In urban areas, where there are many towers, this may give a picture location within a couple hundred feet. In rural areas, towers may be miles apart.


slightly more accurate location picture can be generated by tracking which 120 degree "face" of the tower is receiving a cell phone’s signal.  

A more accurate picture of a phone’s location may be generated by using triangulation, which uses TDOA or AOA to measure the relative signal strength of the three nearest cellular towers. The FCC’s Enhanced 911 (E-911) mandate requires the ability to track 95% of calls within 300 meters using triangulation. This method of tracking is popular with cellular service providers, because it uses the existing infrastructure. And various technologies are being widely implemented that use enhanced methods of triangulation to provide a more accurate picture of the phone’s location.

The use of a GPS chip in the handset of new phones has emerged as an alternative for many cellular service providers. Over 90% of cell phones currently in use have built-in GPS location-tracking capabilities that incorporate longitude and latitude using the already-existing GPS satellite infrastructure, and allow for extremely accurate tracking—potentially within 50 feet. The FCC’s E-911 mandate requires that 95% of 911 calls from cellular phones using GPS can be tracked within 150 meters. GPS suffers in urban areas and when the phone is indoors, because a direct line to the satellite is broken. Assisted GPS (A-GPS) technology, which provides reference points for the system, mitigates this problem and shows promise for the future.

---

29. See S.D.N.Y. I Decision, 405 F. Supp.2d 435, 437 (2005). It does not appear that such “face” information is tracked by all cellular service providers.


32. Note that, despite having widespread GPS-enabled handsets, many service providers will continue to provide 911 location tracking using network-based triangulation. Handler, supra note 6 at ¶ 21.


This sort of electronic surveillance is generally governed by the Electronic Communications Privacy Act of 1986 (ECPA). The ECPA was itself a major overhaul of the Omnibus Crime Control and Safe Streets Act of 1968. These statutes have been frequently amended in an effort to keep up with changes in modern technology and shifting security concerns, and the result is ambiguous, overlapping guidance in the area of cell phone location tracking.

In order to obtain location tracking information, law enforcement must seek a court order requiring the cellular service provider to turn over this data. It appears that these orders are routinely requested by law enforcement, and are probably routinely granted.

However, there is considerable debate regarding the legal standard required for obtaining these orders, depending on what aspect of the ECPA one believes is implicated. As we shall see, location tracking information may be analogized to a pen register (a device whereby law enforcement can track the numbers called by a particular phone) or a trap-and-trace device (a device which allows tracking of the numbers of inbound phone calls). This sort of data is not protected by the Fourth Amendment, and can be obtained on a relatively minimal showing of “certified relevance.” The pen register standard may apply to the signaling and routing information used by cell phones, in addition to phone numbers, however, cell

36. As Magistrate Judge Gorenstein grumbled: “[Analyzing the relevant statutes] has hardly been a satisfying exercise inasmuch as we are left with the conclusion that Congress has given a direction that cell site information may be obtained through some unexplained combination of the Pen Register Statute with some other unspecified mechanism.” S.D.N.Y. I Decision, 405 F. Supp. 2d at 442. Indeed, on relatively similar facts, different district court decisions have come out differently, illustrating the murkiness of the relevant statutes in this area.
37. This is based on the requirements of the ECPA (see note 34, supra). However, it appears that law enforcement has the capability to obtain cell phone location data without the help of the service provider. See S.D. Tex. I Decision, 396 F. Supp. 2d at 755 (discussing a device that can snatch cell phone signals out of the air called a “trigger-fish”).
40. 18 U.S.C. § 3127(3) (2007). Under the Communications Assistance for Law Enforcement Act (CALEA), which amended the ECPA, cell phone tower location information falls under the definition of call identifying information, and has been held to
phone location information may not be obtained pursuant "solely" to a pen register order.\textsuperscript{41}

"Solely" implies that some other authority, when combined with a pen register order, will permit law enforcement to track cell phone location information. However, what that other authority may be is a matter of swirling debate in the federal district courts. Four courts have held that the other authority Congress had in mind is the Stored Communications Act (SCA), which requires a showing of "specific and articulable facts."\textsuperscript{42} However, the majority of district courts that have considered the matter have held that the other authority required is that applicable to tracking devices: the probable cause normally required for a warrant.\textsuperscript{43} The distinction between these two lines of decisions has turned in part on the sort of cell phone tracking information requested, as will be discussed further.

Present statutes do not require that evidence gathered without a court order—in violation of the statute—be suppressed.\textsuperscript{44} Of course, these statutory provisions must satisfy the baselines established by the Constitution. Unfortunately, Fourth Amendment doctrine in this area is more confusing than any existing legislation.\textsuperscript{45}

C. Fourth Amendment Precedent.

Under current doctrine, whether an unreasonable search has occurred is a matter of case-by-case, technology-by-technology analysis.\textsuperscript{46} Though the Supreme Court attempts to give law enforcement "bright-line" rules to follow, the realities of modern life and advancing technologies stretch previous Fourth Amendment parameters. Though no direct analogue to cell phone location

\begin{itemize}
  \item \textsuperscript{41} 47 U.S.C. § 1002(a)(2) (2007).
  \item \textsuperscript{42} 18 U.S.C. § 2703(d) (2007).
  \item \textsuperscript{43} The standard required for tracking device surveillance is codified at 18 U.S.C. § 3117. The probable cause required is spelled out in Fed. R. Crim. Proc. 41.
  \item \textsuperscript{44} As long as such statutes are constitutional, they do not violate the Fourth Amendment, and the exclusionary rule does not apply.
  \item \textsuperscript{45} See Anthony G. Amsterdam, \textit{Perspectives on the Fourth Amendment}, 58 MINN. L. REV. 349, 349 (1974). Few would argue that Fourth Amendment jurisprudence has gotten any clearer in the last 30 years.
  \item \textsuperscript{46} See Kyllo v. United States, 533 U.S. 27 (2001), Dow Chemical Co. v. United States, 476 U.S. 227 (1986), and Katz v. United States, 389 U.S. 347 (1967) (involving thermal imaging, high-powered cameras, and sophisticated eavesdropping equipment, respectively—each stretching the applicability of existing doctrine).
\end{itemize}
tracking has been considered by the Court, two lines of cases raise similar issues. 47

*Smith v. Maryland* 48 considered the warrantless use of a pen register by law enforcement. The Court held that in dialing a phone number, the individual voluntarily conveys the number to the phone company, and thereby assumes the risk that this information will be revealed by the phone company to the police. 49 As will be discussed below, this information is similar to cell phone location information, which is conveyed by the cell phone to the cell phone service provider. 50

*United States v. Knotts* 51 and *United States v. Karo* 52 analyzed the use of electronic tracking beepers without a warrant. In those cases, law enforcement officers placed a radio transmitter inside a five-gallon drum of chloroform, and a five-gallon can of ether, respectively, before those containers were sold to the defendants, who used the chemicals for the manufacture of illegal drugs. Where the tracking beeper was used to follow the movements of the defendants on public thoroughfares, the Court found no violation of any reasonable expectation of privacy, for both a car and its occupants are in plain view on open roads. 53 However, in *Karo*, when the beeper was used to ascertain the location of the container inside a house, the Court found the search to be unreasonable, because such information could not have been visually verified from outside the house. 54 As will be discussed below, cell phones share some

47. The applicability of these two lines of cases to cell phone tracking has been noted in Matthew Werdegar, *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 STAN. L. & POL’Y. REV. 103 (1998) and Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381 (2003). Recent district court decisions recognize the applicability of these two lines of cases as well.

49. *Id.* at 744-45. This “assumption of the risk” holding was built on cases such as *United States v. Miller*, 425 U.S. 435, 443 (1976), which held that an individual has no expectation of privacy in financial information voluntarily conveyed to a bank. See generally Patricia L. Bellia, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & The USA Patriot Act: Surveillance, Records & Computers: Surveillance Law Through Cyberlaw’s Lens*, 72 GEO. WASH. L. REV. 1375 (2004).
50. *See infra* Part III B.
54. *Karo*, 468 U.S. at 715 (1984). Indeed, even that which may be ascertained from outside the house may be considered an unreasonable search, if the method of the search reveals too much about the interior of the house. *Kyllo*, 533 U.S. at 34.
similarities with tracking beepers, but are also distinct in a number of ways.

A cell phone is not exactly like a pen register or a tracking beeper. The applicability of either line of cases depends on a number of factors. One factor is the precise type of location data sought: whether the data is historical or “real-time” data; whether the data is gathered only when the phone’s user initiates a call, or at any time the phone communicates with cellular towers; and the level of specificity of the location data being gathered. A second factor depends on where the suspect is when his cell phone is tracked. A third factor is determining the proper focus of analysis: focusing on the location of the phone itself, or on the user of the phone.

III. Applying the Fourth Amendment to Cell Phone Location Tracking.

A. Historical Data Versus “Real-time” Data.

Cell phone location data is routinely tracked by cell phone service providers, both so that wherever a user is he will quickly receive an incoming call, and because each call must be logged for billing purposes. Law enforcement may obtain this data concurrently—that is, as it happens in real time. When law enforcement requests real-time data, it must ask the court for a prospective order because such real-time data is inherently not yet in existence at the time of the request. Alternately, in some circumstances, law enforcement may go through the retained records of the service provider to reconstruct a picture of where a suspect was at a given time in the past.

The distinction between historical and real-time cell phone location data matters for a number of reasons. However, in one respect, the distinction is largely meaningless. Historical data may be recorded, compiled, and transmitted to law enforcement so quickly as to effectively operate as real-time data. Where historical data operates as real-time data, courts should treat the data as such.

55. But see D.D.C. Decision, 407 F. Supp. 2d 134, 135 (2006) (noting the concern that if a warrant is required to obtain real-time data, Fed. R. Crim. Proc. 41 and the Fourth Amendment require “probable cause to believe that the information sought is itself evidence of a crime, not that the information is relevant to an investigation.” Where information is sought that hasn’t yet happened, it is difficult to argue that it is “itself evidence of a crime.”).

56. Indeed, in a number of district court decisions, the government has argued that real-time location information falls under Stored Communications Act, 18 U.S.C. §
To the extent truly historical data is utilized by law enforcement, other issues arise. Truly historical data allows police to reconstruct the past whereabouts of a suspect; this type of data is distinct from the real-time tracking utilized in the tracking beeper cases. Truly historical data may qualify as a business record, and accordingly, would receive very limited Fourth Amendment protection under the “assumption of the risk” doctrine. Truly historical data may also be better able to meet requirements of a warrant, and would not run afoul of the Court’s historical concerns with prospective surveillance.

In addition to being more limited than real-time tracking by only providing evidence of that which has already happened, historical data is limited in another way. It is unlikely that cellular service providers record the location of each registration—which occurs many times per minute—of every cell phone every hour of the day. The amount of data this would generate is immense, and there is little practical incentive for service providers to keep this data. However, if location-based marketing takes off, there may be a strong financial incentive for service providers to keep this information. Additionally, the cost of data storage continues to shrink over time. While impractical today, reconstructing a person's whereabouts via historical cell phone records may not long be the province of science fiction.

Real-time data is a more penetrating form of surveillance, which is clearly more desirable to law enforcement, and of greater concern to privacy advocates than historical data. The Supreme Court has

2703(c)-(d). See E.D.N.Y. Decision, 396 F. Supp. 2d at 312-14 (discussing, and rejecting, the “instantaneous storage” theory advanced by the government). While all data is historical in some sense, when effectively used in real-time it is disingenuous to treat it as a historical record.

57. Reconstructing someone's whereabouts through phone records is not analogous to following them on a public street, which was the basis for the holding of Knotts. See Werdegar, supra note 47 at 109.

58. See Miller, 425 U.S. at 443. The Stored Communications Act, which deals with historical communication records, reflects the weakened protection afforded business records by allowing for a court order to issue based on a showing of “specific and articulable facts showing . . . [that the information sought is] relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d).


60. See Berger v. New York, 388 U.S. 41, 59 (1967) (construing a two-month eavesdropping authorization as permitting a “series of intrusions, searches, and seizures pursuant to a single showing of probable cause.”).

61. See, e.g., Jonathan Krim, supra note 38, at A5. Although using cell phone location tracking technology to preemptively fight crime is some ways off, real-time tracking clearly can be applied today to solve ongoing crimes such as kidnapping and to track
considered real-time tracking only in the context of the tracking beeper cases. There, the Court had no problem with real-time tracking, as long as it took place in public places, and the Court equated beeper tracking to an agent physically following a suspect. In this respect, real-time tracking with a cell phone is little different from real-time tracking with a beeper, or in person.

But the analogy to an agent following a suspect does lose some of its force when applied to cell phone location tracking. If cell phones are considered tantamount to tracking beepers, then 200 million Americans are carrying tracking beepers. The scope of such a proposition gives one pause. The practical impediments to having agents following 200 million Americans 24 hours per day suggests that the analogy to physically following suspects in person is inapposite. Moreover, if two-thirds of all Americans were aware that they had police tracking beepers in their cars, or were regularly followed by police, one might expect both a titanic shift in privacy expectations, and an outcry from the public. And yet, if the analogy between tracking beepers and cell phones is carried to its logical conclusion, we are all carrying tracking devices and, at least while we are in public, the Fourth Amendment is not implicated. This goes well beyond any sort of “sense-enhancement” as condoned in Knotts, to borderline omniscience.


63. Indeed, we all may be deemed to have consented to carrying a tracking beeper with us, knowingly or unknowingly. See S.D.N.Y. I Decision, 405 F. Supp. 2d at 449 (“[T]he Government does not seek to install the ‘tracking device’: the individual has chosen to carry a device and to permit transmission of its information to a third party, the carrier”). Under the “reasonable expectations” test, this “voluntary consent” may actually receive less judicial concern than a tracking beeper, which is installed without the knowledge nor the consent of the suspect.

64. Presumably, given the investment of personnel in physically following a suspect, some fairly high degree of suspicion must be involved. And though tracking beepers make following a person much easier, such beepers (at least the ones considered in Knotts and Karo) require the transmitter to be relatively near to the receiver. Additionally, the installation process requires some sort of focused suspicion to make the tracking worthwhile.

65. Similar fears of widespread surveillance without judicial oversight were raised in Knotts, and were curtly dismissed, for “the fact is that the ‘reality hardly suggests abuse . . . .’” Knotts, 460 U.S. at 283 (citation omitted). However, without judicial oversight, it becomes rather difficult to ascertain whether the reality of such surveillance suggests abuse.
B. Passive Versus Call-based Location Tracking.

Cell phones constantly communicate with the towers around them. This occurs passively on one channel as long as the phone is powered on, with no action taken by the phone’s user. The only way to stop this passive communication is to turn the phone off.

Call-based location tracking occurs on a separate channel only when the phone’s user initiates or receives a call. The caller is clearly conveying his location to the phone company in order to complete his call, and thus it appears that call-based location tracking falls within the ambit of Smith v. Maryland.

Three distinctions may be raised here. First, a home phone is generally used by the people who live in the home—often more than one person. Cell phones are virtually always used by only one person—the owner. Thus law enforcement is given a more particular set of data than under the facts of Smith.

A second distinction is that using a pen register or trap-and-trace device, law enforcement only receives the phone number dialed or received, with little additional information. Generally a pen register is sought because law enforcement is interested in knowing whom a suspect is calling. Any location information that may come with a pen register (such as knowing that the suspect is at his home when he makes a call) is purely incidental. Cell phone location information, on the other hand, is not incidental—instead, the suspect’s location is precisely the information sought.

Nonetheless, the Smith court did not seem particularly concerned with the type of data sought, as long as it was not “content.” Rather, the holding rested on the “assumption of the risk” premise: the data had been conveyed to a third party; thus, there was no longer any expectation of privacy in it. Applying assumption of the risk, it appears at first blush that a cell phone caller can have no expectation of privacy in his location when he initiates or receives a phone call.

66. See supra Part II A.
67. Under the Communications Assistance for Law Enforcement Act (CALEA), cell phone tower location information falls under the definition of call identifying information. See supra note 40.
68. See Dawn Nafus & Karina Tracey, Mobile Phone Consumption and Concepts of Personhood, in PERPETUAL CONTACT: MOBILE COMMUNICATION, PRIVATE TALK, PUBLIC PERFORMANCE, supra note 3, at 212.
69. For a discussion of how slippery the concept of “content” as opposed to call identifying information really is, see David McPhie, Almost Private: Pen Registers, Packet Sniffers, and Privacy at the Margin, 2005 STAN. TECH. L. REV. 1.
70. In distinguishing the information requested in its decision from prior district court decisions, the S.D.N.Y. I Decision noted that law enforcement had only requested data
Third, the assumption of the risk applied in *Smith* was premised on an assumption by the court that the phone's user was aware that he must convey phone numbers to the telephone company to complete calls, and that records may be kept of those calls.\(^7\) Cell phone users may, on the whole, be unaware that their phones continually broadcast their location, despite any action on the part of the user.\(^7\) This provides some differentiation from *Smith*; however it is very likely that in the near future the majority of the populace will be aware that their phones passively convey location signals.\(^7\) Indeed, the Supreme Court has consistently assumed a high degree of awareness—and thus a lack of privacy expectations—by the public of such technologies as helicopter fly-overs\(^7\) and high-powered cameras.\(^7\) This assumption finds further force in the fact that cell phones are in widespread general public use.

Passive location tracking requires no great leaps in logic to fall within the holding of *Smith*. There is no real positive action by the phone's owner; however, his phone is conveying his location to a third party all the same and, if he is aware of the underlying technology, he is thereby assuming the risk. He has the option of turning his phone off completely.\(^7\)

One court has hinted that passive location tracking is particularly insidious. In *United States v. Forest*,\(^7\) a DEA agent called the defendant's phone a number of times without letting it ring, in order

\(^{71}\) Smith v. Maryland, 442 U.S. 735, 742 (1979).

\(^{72}\) See W.D. La. decision, 411 F. Supp. 2d at 682 (presuming that because cell phone users have likely experienced dropped calls, they are aware that their cell phone communicates with the nearest tower, and that because cell phone users have likely experienced roaming, "users know that third party service providers are aware of their general location vis-à-vis the nearest tower, at the beginning of, during and at the end of each call.").

\(^{73}\) See infra note 94 (suggesting that a substantial segment of the populace is already aware of the location-based functionality of cell phones). Particularly as more location-based functions become available on cell phones, the assumption will become increasingly tenable that the majority of the population is aware that cell phones communicate their position back to the service provider.


\(^{75}\) Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

\(^{76}\) Though discussing only call-based location tracking, the court in the W.D. La. Decision suggested that the phone's user always had the option to turn the power off on the phone. 411 F. Supp. 2d 678, 682 (2006).

\(^{77}\) 355 F.3d 942 (6th Cir. 2004).
to track his location. In dicta, the Sixth Circuit indicated that the agent caused the defendant’s phone to send out signals, and that the defendant did not voluntarily convey any signals himself, suggesting that such a search might fall outside the rationale of Smith. However, it is technologically possible to track a suspect without actually calling his phone, as his phone is constantly sending out signals. Turning off the phone is the only way to stop conveying one’s location to the phone service provider, though from a practical standpoint the option to turn the phone off hardly seems like an option, as it strips the phone of its ability to receive calls.

C. The Level of Specificity of Location Data Gathered.

Varying technologies provide different levels of specificity in location information. Traditional Cell ID tracking can position an individual only within 250 meters at best. U-TDOA, an enhanced form of traditional triangulation, can provide a location within 50 meters. A-GPS may get as close as 30 meters, although it suffers indoors and in urban areas. Undoubtedly, as technology develops, location tracking will become more precise.

In earlier district court decisions, law enforcement requested real-time cell site information and was uniformly denied. In more recent cases, law enforcement has requested only the location of the nearest tower to the suspect. Magistrate Judge Gorenstein of the Southern District of New York held that this brought the case squarely under the precedent of Smith, and that the beeper tracking cases were inapposite. Magistrate Judge Hornsby of the Western

78. Id. at 951. In Smith, the suspect initiated all calls that were tracked.
79. See An Examination of U-TDOA and Other Wireless Location Technologies, note 30, supra.
80. Id.
81. "Many of the initial applications for cell site information sought information that could be used for triangulation. After these applications were rejected by many courts, however, the government began to request information regarding only one tower at a time, apparently in the hope that applications for less detailed and invasive information would meet with a warmer judicial reception." S.D.N.Y. III Decision, 460 F. Supp. 2d 448, 452 (2006).
82. Knowing the location of one tower is clearly less useful than knowing the relative positions of three towers; however, seeking authorization for only one tower perhaps makes a more colorable statutory argument that the cell phone is not being used as a tracking device; rather, only signaling information is sought, arguably bringing the information desired within the Pen Register Statute (18 U.S.C. § 3127(3)).
83. S.D.N.Y. I Decision, 405 F. Supp. 2d 435, 449-50 (2005). The court viewed this as the voluntary provision of data to a third party, governed by Smith, and did not view this sort of data as location-tracking data. The later S.D.N.Y. III Decision was more equivocal, recognizing the applicability of both the beeper tracking and pen register cases,
District of Louisiana similarly held that because the data sought was relatively imprecise, the analogy to tracking beepers failed, as "the user's movements will not be tracked in the strict or literal sense of the word." 84

Learning only the location of the nearest tower provides a more general picture of the suspect's location. Nonetheless, it gives an approximate idea of where the suspect is. In urban areas, where towers can be within a few hundred feet of each other, knowing the location of the nearest tower may be more precise than basic triangulation.

Magistrate Judge Hornsby reasoned that because the location of the nearest tower cannot reveal with pinpoint precision whether or not, as in Karo, someone is in a home, the Fourth Amendment was not implicated. But it is unclear why there should be a constitutional distinction based on tracking precision. Tracking someone is tracking someone, and there is no logical reason the principles applied should change based on whether a general or more specific picture of the suspect's whereabouts is available.

Indeed, tracking someone's location less specifically increases the chances that one is being tracked while in a private area, such as the home. Though law enforcement may not know that the suspect is in his home, they may nonetheless be unwittingly tracking his location while he is in his house—raising significant Fourth Amendment concerns. And such tracking clearly discloses a suspect's general vicinity, revealing what state and town a person is in, and, in denser areas, even more particular data.

D. Tracking the Suspect at Home.

In theory, under Katz, the Fourth Amendment protects people and not places. 85 However, in the beeper tracking cases, the Court's emphasis was not on protecting the person, unless the person was in his home. 86 The Court's most recent technology-based surveillance case, Kyllo v. United States, re-emphasized the sanctity of the privacy of the home. 87

but refusing to reach the constitutional issue in the abstract. 460 F. Supp. 2d 448, 462 (2006).

87. 533 U.S. 27, 34 (2001) ("[I]n the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy
This presents a major problem in the context of cell phone location tracking. Cell phones are constantly in and out of private places—most commonly homes—where no law enforcement agent could intrude without a warrant. It would be extremely difficult to track a suspect via cell phone only while he was outside the home, but never while he was inside the home. This implication of the home suggests the need for a warrant to engage in cell phone tracking.

However, unforeseen advancements in technology may make such particular, outside-only tracking feasible. Further, there is little need to track a person when he is in his home if law enforcement is simultaneously maintaining visual surveillance. Such surveillance will generally reveal whether a person is home or not, and if one knows that a person is in his home, what is the need to track his whereabouts? Simply turn off the tracking mechanism when the suspect enters his house, and turn it on again when he leaves. This would limit the economic efficiency of cell phone tracking by requiring some in-person visual surveillance, thus limiting the potential for indiscriminate searches by requiring some particularized suspicion on the part of law enforcement.

E. Focus on the Phone Versus the Suspect.

In the beeper tracking cases, the Court appeared to focus not on the beeper itself, but on the suspect. The Court was unconcerned with any invasion of the defendant's property, and rather viewed the beeper as simply another way to follow a person around. This method—focusing on the person, and not the thing being tracked—may translate to cell phones as well, which are generally tied to one person.

However, in the beeper tracking cases, the Court also noted that visual surveillance would readily reveal when a 5-gallon drum was brought into or out of a house or car. The same cannot be said of cell phones: they are small enough that, unless they are in use, visual

---

88. Payton v. N.Y., 445 U.S. 573, 590 (1980) ("[T]he Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant.").

89. United States v. Knotts, 460 U.S. 276, 285 (1983) ("A police car following Petschen at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin owned by respondent, with the drum of chloroform still in the car.").

90. See Nafus & Tracey, supra note 68.
surveillance often cannot reveal where the phone is. Focusing scrutiny on the phone, and not the user of the phone, would mean that law enforcement would often be affecting a virtual pat-down, determining the whereabouts of a phone that cannot be seen with the naked eye. As a person’s “effect,” the phone should be entitled to Fourth Amendment protection itself,\(^9\) and a virtual search of the phone would likely be held unreasonable.\(^9\) As Justice Stevens, concurring in *Karo*, recognized, “[c]oncealment of personal property from public view gives rise to Fourth Amendment protection.”\(^9\)

**IV. Cell Phone Location Tracking is an Unreasonable Search.**

The question of whether cell phone location tracking constitutes a reasonable search is at best unclear. Indeed, different district courts have come out differently on very similar facts. However, on closer scrutiny it seems likely that cell phone location tracking constitutes an unreasonable search. Three fundamental aspects of Fourth Amendment jurisprudence suggest that cell phone location tracking is unreasonable.

**A. Assumption of the Risk is Limited.**

As discussed above, the difference between tracking the location of a cell phone when a call is made, versus tracking a cell phone passively at any time is not a constitutionally-based distinction. Though call-based tracking may appear to mirror the analysis of *Smith*, it is a surface similarity. Unlike *Smith*, the information being sought is the suspect’s location, and not the phone number or “routing” information involved. In this way, call-based tracking and passive location tracking both reveal the same sort of information.

To apply *Smith* to both passive and call-based location tracking, one must assume that most people realize their location may be tracked and have thus assumed the risk of being tracked. Many Americans may be unaware today that their location can be tracked with their cell phones, and thus have not assumed the risk of having their locations tracked. However, as location-based services grow,

---

\(^9\) U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.”).

\(^9\) Absent suspicion of a weapon, such a frisk could not be sustained under *Terry v. Ohio*, 392 U.S. 1 (1968).

public awareness of those services will grow, along with some recognition of the underlying technology. 94

But even a surge in awareness of the location-tracking capabilities of cell phones does not mean that we will all be deemed to have assumed the risk of being tracked because the assumption of the risk doctrine is qualitative in nature. Not everything that is disclosed to others is deemed to have been risked. This was recognized in the very holding of Smith: though both the content of the call and the number dialed were both transmitted to the phone company, only the number dialed was deemed “risked” by the caller. Any search of the content of the call would have fallen within the purview of Katz, and would clearly have been an unreasonable search. 95

The limits of the assumption of the risk doctrine are unclear. Where one broadcasts something to the world, one may rightly be said to have assumed the risk that others will discover it. However, if anything that has been divulged to a third party may be deemed “risked,” then we would all be lacking the most basic privacy. Modernly, most important data about individuals is held by third parties. 96 One voluntarily conveys intimate financial, medical, and even psychological data to our banks, doctors, and counselors. While some of this data may be obtained without a court order, 97 much of it may only be obtained with judicial oversight. 98 What risks one assumes appear to depend in large part on the intuition of the justices. Certain things, though they may be known by third parties,
are so private in nature that they are more akin to the content of a phone call than the mere routing information of the call.

The Court wrestled with the nuances of what sort of risks we assume in the modern world in *Kyllo v. United States*. In *Kyllo*, law enforcement used a thermal imaging device to track the heat emanating from the defendant’s home. Heat tracking disclosed that certain portions of the defendant’s home were far hotter than the rest of the home, indicating that the defendant was likely growing marijuana indoors. On the basis of this imaging scan, a warrant was obtained and the home was searched, resulting in the defendant’s arrest.

The dissent argued that the defendant had assumed the risk that any passerby might discern a greater amount of heat emanating from certain parts of the home. It was incumbent upon the defendant to “make sure that the surrounding area is well insulated” if he wanted to conceal what was going on indoors.

The majority, however, recognized that allowing technology to search the home in ways previously unimagined threatened to “leave the homeowner at the mercy of advancing technology.” To suggest that, in order to maintain privacy in the face of advancements in technology, one must now add extra insulation to one’s home struck the majority as flatly unreasonable.

Similarly, in the case of cell phones, the only option for evading tracking is to turn off the cell phone, or at minimum to not make or receive any calls. But turning off the phone strips the phone of the ability to receive inbound calls, and protecting oneself by not using the phone simply fails to recognize the reality of cell phone usage in modern life. “It is idle to speak of ‘assuming’ risks in contexts where, as a practical matter, individuals have no realistic alternative.”

The logical extremes of assumption of the risk were rejected in *Kyllo*, and this limitation on assumption of the risk should also be recognized in the case of cell phone location tracking.

B. Property Precepts Remain Prominent.

As discussed above, tracking a suspect less specifically by utilizing only the location of the nearest tower instead of triangulation

100. Id. at 30.
101. Id. at 45 (Stevens, J., dissenting).
102. Id. at 35.
or GPS tracking is not a constitutional distinction. Indeed, less-specific tracking may implicate greater Fourth Amendment concerns, as the suspect may more easily—if unintentionally—be tracked in a private location such as the home. More specific tracking may well be desirable, so that expectations of privacy in the home are not trampled.

That expectation of privacy in the home has long been recognized by the Court, and has been affirmed in *Kyllo* and recently in *Georgia v. Randolph.* *Randolph* dealt with the issue of whether one tenant may consent to a search of the home despite the clear denial of consent to a search by a fellow cotenant. The Court held that the consenting tenant could not override the cotenant's denial of consent, grounding its ruling in "the centuries-old principle of respect for the privacy of the home."

The Court has been firm that technology may not shrink the privacy afforded by the home. If thermal surveillance of a home is unreasonable, tracking an individual when he is in his home should likewise be found unreasonable. And if the home—and presumably other places, such as hotel rooms and phone booths, which have been analogized to the home—are off-limits, it is difficult to envision a form of cell phone location tracking that would survive a constitutional challenge.

**C. Reasonable Expectations Have Subtly Shifted.**

It would initially appear that as the majority of Americans become aware that their location may be tracked through their cell phones, they will be deemed to no longer have a reasonable expectation of privacy in their location. To expect to be untracked when one knows one may be tracked is simply an unreasonable expectation.

---

104. "The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." *Silverman v. United States*, 365 U.S. 505, 511 (1960) (citing *Entick v. Carrington*, 19 Howell's State Trials 1029 (1765), and *Boyd v. United States*, 116 U.S. 616 (1885).
107. *Id.* at 1519.
108. *Id.* at 1523 (quoting *Wilson v. Layne*, 526 U.S. 603, 610 (1999)).
Traditionally, the test taken from *Katz* queries whether the subject of the search had a reasonable expectation of privacy. This method of analysis can be problematic, for any expectation of privacy may be shrunken if, for example, the government broadcast that “we were all forthwith being placed under comprehensive electronic surveillance.” The reasonable expectations test focuses on the expectations of the individual, which is problematic because “the regulation of police behavior”—protecting of the people from unreasonable searches and seizures—“is what the Fourth Amendment is all about.”

The recent cases of *Kyllo* and *Randolph* illustrate that the Court’s application of “reasonable expectations” may be shifting. In both cases, the Court recited a form of the “reasonable expectations” test. In *Kyllo*, the Court cited the traditional reasonable expectations test from *Katz*, and applied it to the home. In *Randolph*, the Court queried “the great significance given to widely shared social expectations” of privacy in making a determination of the reasonableness of the search.

But in neither case did the Court isolate its focus on the actions of the individual; rather, the Court focused on the conduct of the police officers. In *Kyllo*, the Court held that when police use “a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search.’” In *Randolph*, the Court held that a disputed consent to search the home “gives a police officer no better claim to reasonableness in entering than the officer would have in the absence of any consent at all.” The Court did not overlook the individual in either case: in both cases the individual was in his home, and thus was deemed to have a reasonable expectation of privacy. But the Court did not stop with analyses of the individuals’ expectations, and scrutinized the reasonableness of law enforcement as well.

This shift in the Court’s analysis suggests that society’s expectations of what constitutes a reasonable search may play a part in determining the reasonableness of a search. A test focused solely on the individual’s expectations allows advances in technology to
squeeze expectations, leading to a "downward spiral in Fourth Amendment protection." But a test based on societal expectations of what government can and cannot reasonably do may very well lead to greater protection of privacy.

It is difficult to assess societal expectations. Some citizens would undoubtedly be willing to allow warrantless cell phone location tracking in order to combat crime and terrorism. Others would find such tracking Orwellian and anathema to a free society. Where a solid societal expectation of privacy exists - as in the home—it seems clear that a cell phone location search is unreasonable. However, it remains to be seen how the Court will address shifting societal expectations as location-tracking technologies become more common.

V. Conclusion

Fitting the unique attributes of cell phone location tracking into existing Fourth Amendment precedent is something like fitting a round peg in a square hole. Location information—whether tracked passively or only when calls are made—is qualitatively different from the routing information at issue in Smith. And as cell phones are voluntarily carried by the majority of Americans, cell phone tracking is much different as a practical matter from the tracking devices at issue in Knotts and Karo.

Nonetheless, these two lines of cases counsel that cell phone location tracking is an unreasonable search. First, as reflected in Karo and repeatedly confirmed by the Supreme Court, any warrantless surveillance of an individual in his home is unreasonable. Cell phone location tracking—at least with presently-existing technology—cannot help but implicate the home. Second, assumption of the risk is a nuanced doctrine. Individuals should not be required to take unreasonable protective measures to keep private that which they reasonably expect to keep private. Assertions that individuals wishing to avoid location tracking should turn off their phone or leave it at home are unreasonable in light of modern cell phone usage patterns.

Finally, the beginnings of a shift in the core application of the reasonable expectations test also suggest that cell phone location tracking is an unreasonable search. Recent Supreme Court decisions have focused not only on the suspect's reasonable expectations of

privacy, but on the reasonableness of the actions of law enforcement. This shift in analysis potentially offers Fourth Amendment protection to cell phone users in a world where cellular location-based services are becoming increasingly widespread.