CAN POLICE TRACK YOUR WIRELESS CALLS? CALL LOCATION INFORMATION AND PRIVACY LAW

LAURIE THOMAS LEE, PH.D.

INTRODUCTION

Cellular telephone location tracking technology came to the rescue several years ago in the United Kingdom when criminals kidnapped a Greek magnate, holding him for ransom. Although the criminals tried to confuse the police by using two mobile phones that they moved around, police were eventually able to track them using cellular base station triangulation data.[1] In the United States, however, a woman, whose car had skidded off a Florida turnpike into a canal, called 911 on her cell phone, but rescue units could not determine her precise location. By the time authorities found her, she was dead.[2]

To help prevent such tragedies, cellular providers in the United States are now required to begin providing location-based information that can pinpoint the location of a wireless phone making a 911 emergency call. Federal Communication Commission (FCC) Enhanced 911 (E911) rules require carriers to be able to provide precise location information by 2003,[3] and have a fully implemented wireless call location system in place by December 31, 2005.[4] Although cellular service providers already keep track of cell site location information for purposes of billing and assessing roaming charges, these E911 requirements call for more detailed location information and subsequent disclosure to emergency service providers.

Such advanced call location information technology certainly promises a wealth of benefits. The information potential in mobile commerce (m-commerce) is a commercial dream for advertisers who may see a mobile location services market worth $20 billion by

---

[1] *See* Steve Gold, *Privacy Storm Brewing Over Mobile Phone Location Tech.*, COMPUTER USER, *at* http://www.computeruser.com/clickit/printout/news/310295880003251200.html (Nov. 13, 2000).

[2] *See Your Phone Knows Where You Are*, POPULAR SCI., Oct. 12, 2002, http://www.popsci.com/popsci/science/article/0,12543,266052,00.html [hereinafter *Your Phone Knows*].

[3] *See* In the Matter of Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, Order to Stay, Fed. Comm. Comm'n, CC Docket No. 94-102, July 26, 2002 [hereinafter In the Matter of Revision, Order to Stay].

[4] *Id.*

2006.[5] Subscribers to developing location services may access driving directions,[6] local news or weather, traffic delay information, and so-called "concierge services"[7] that determine the location of nearby restaurants and theatres.[8] Call location information will also aid in law enforcement, not only in assisting citizens calling 911, but also in tracking drug dealers and locating stolen vehicles and escaped felons. In fact, Global Positioning System (GPS)[9] technology is already being used in 20 states to monitor convicted criminals on probation, parole, home detention, and work release.[10]

But just as Americans have come to enjoy the freedom of movement associated with cell phones, they may find their own phones have effectively become ankle bracelets. While location tracking capabilities offer considerable public safety protections, the information available also presents greater opportunities for unrestrained government monitoring and misuse. As law enforcement agencies take advantage of this efficient investigative opportunity—as is already done in Europe,[11] Americans will realize less personal privacy, tilting the delicate constitutional balance between

---

[5] *See Mobile Location Services Driven by M-Commerce Will Generate $20 Billion by 2006, Study Says*, WIRELESS NETWORKS ONLINE NEWS, *at* http://www.mobileinfo.com/News_2001/Issue04/Ovum_location.htm (Jan. 15, 2001) [hereinafter *Mobile Location*].

[6] The most conspicuous current example of location technology is General Motor's OnStar service, which can automatically locate a car and call for assistance when a subscriber's car breaks down. *See* Tod Newcombe, *Supplement: Who's Tracing Your Steps?*, GOV'T TECH., *at* http://www.govtech.net/magazine/sup_story.php?magid=17&id=5766&issue=9:2001 (Sept., 2001).

[7] *See* Maureen Fab, *Location Tracking Has Its Drawbacks, Appeal*, ITS AMERICA NEWS, *at* http://www.itsa.org/itsnews.nsf/$All/3005DB9813769E5785256C670049C3BB?OpenDocument (Nov. 4, 2002).

[8] The privacy implications for nongovernmental interceptions and disclosures of location information is a very real and growing concern. But the extent to which cellular carriers can use and forward this type of calling party number identification (CPNI) to commercial interests and others is unfortunately beyond the page limit and hence scope of this analysis.

[9] GPS is a series of 24 satellites, originally launched by the Pentagon to aid military operations. The arrival times of several satellite signals can be used to compute longitude and latitude. *See Your Phone Knows*, *supra* note 2.

[10] David Sevitt, *No Place: Global Positioning Systems Technology is a Helpful Consumer Tool, but it's Also an Invisible Surveillance System, and That Has Some Privacy Advocates Worried*, OTTAWA CITIZEN, Aug. 29, 2002, LEXIS, News Library.

[11] *See* Gold, *supra* note 1; *see also Mobile Location*, *supra* note 5. Authorities in Switzerland have also traced the movements of some mobile phone users, causing concern. *See* Stephen Bouvet, *Swiss Citizens Upset at Report Saying Police Have Tracked Cellular Phone Users*, MOBILE PHONE NEWS, *at* http://www.findarticles.com/cf_0/m3457/v15/20218329/print.jhtml (Jan. 5, 1998). The Council of the European Union has considered a proposal that would require all EU countries to retain information on users' online activities and location for one to two years in order to aid in criminal investigations. *See EU Considering New Internet Surveillance Requirements*, PRIVACY INT'L, *at* http://www.privacyinternational.org/issues/tapping/ (Aug. 20, 2002).

liberty and law enforcement.[12]

To what degree the government will utilize call location information is unknown. But the FBI has already created other high-tech surveillance operations such as "Carnivore," which captures and tracks email and web communications, and "Echelon," a worldwide satellite surveillance system that listens for key words and phrases such as "bomb" and "kill the president."[13] Law enforcement officials have also asked the FCC for easy access to cell phone location information.[14] Yet whether or not government agents are necessarily restricted from accessing call location information in the first place is unclear.

To what extent is call location privacy protected? Is there a constitutional right to location privacy? Do existing statutory laws limit government access and protect callers from unrestrained law enforcement monitoring?

This article explores the issues and rights associated with call location privacy. Part I discusses the technology and the FCC's E911 requirements for location disclosures. Part II then examines the state of the existing law by exploring call location privacy rights under the U.S. Constitution. Then in Part III, existing statutory law is scrutinized for its applicability to call location privacy interests and the extent to which law enforcement may monitor and seize location call data. Finally, Part IV presents legislative solutions for clarifying and bolstering call location privacy rights.

I. FCC E911 Rules and Call Location Information Technology

Over 140 million Americans are wireless subscribers,[15] with that number expected to increase to 177 million by 2005.[16] In fact, experts estimate that by 2005, there will be over 1.26 billion wire-

---

12 Compared to the privacy uproar over wired Internet communications in recent years, privacy concerns over wireless communications are expected to be "exponentially bigger." *See* Matt Hamblen, *Slippery Road Ahead for Wireless Location Apps*, Computerworld, Oct. 2, 2000, *at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO51710,00.html.

13 *See* Ephraim Schwartz, *FBI Phone Tapping and Locating Cell Phones Making 911 Calls: Is it Privacy or Paranoia?*, Infoworld, Jan. 15, 2001, at 52.

14 Chris Oakes, *FBI Eyes Easier In for Wireless*, Wired News, *at* http://www.wired.com/news/technology/0,1282,13811,00.html (July 17, 1998).

15 *See* Ben Charny, *Cell Phone Tracking Raises Privacy Issues*, CNet, *at* http://news.com.com/2102-1033-846744.html (Feb. 27, 2002).

16 *See* Ruth Nelson & Martin Keane, *Do You Know My Location? Privacy, E-Personalization and the Smart Phone*, PriceWaterhouseCoopers, *at* http://www.pwcglobal.com/extweb/manissue.nsf/DocID/A0288B37CF54FE1985256A64004A3D04 (last visited Nov. 7, 2002).

less phone users around the world.[17] What was once the "wired nation" is fast becoming the "wireless world," with not only traditional cell phones in use, but also all kinds of wireless devices such as personal digital assistants and laptops equipped with wireless cards.

With so many cell phones and other wireless devices in use, it was just a matter of time before the demand for wireless 911 emergency capability would require service providers to bring their systems in line with wire line 911 service. Indeed, over 200,000 emergency calls come from cell phones every day,[18] or approximately 25 percent of all 911 calls.[19] Yet, until the FCC began creating rules,[20] calls made to 911 from a cell phone did not forward the caller's phone number—much less information about the location of the caller—to an emergency services provider or *public safety answering point* (PSAP). Operators had to expend precious time talking to callers to determine their whereabouts, tying up the system, slowing emergency response time, and potentially getting help to callers too late.

The FCC's finalized E911 rules in December of 1997 required cellular service providers to upgrade their systems in two phases.[21] In Phase I, wireless carriers would have to forward all emergency calls to an appropriate PSAP and provide it with the telephone number of the caller (so that a return call could be placed if necessary), as well as identification of the cell site or base station receiving the call. While the resulting location information would hardly be precise, Phase I requirements would at least allow 911 operators to roughly locate the caller. These relatively simple conditions were to be completed by November of 1998, but the FCC granted an extension to June of 2000.[22]

Under Phase II, cellular service providers have been faced with the more difficult and expensive challenge of having to possess the

---

17 Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices, filed Nov. 22, 2000, at 3.

18 *See Your Phone Knows*, *supra* note 2.

19 *See* Jeff Finkelstein, *Your Cell Phone Tracks Your Every Movement*, Customer Paradigm Solutions, *at* http://www.customerparadigm.com/article-cell.htm (July 11, 2002).

20 Work on these rules began in 1996. *See* In the Matter of Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Call Systems, Report and Order and Further Notice of Proposed Rulemaking, Fed. Comm. Comm'n, CC Docket No. 94-102, July 26, 1996.

21 *See* In the Matter of Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Call Systems, Memorandum Opinion and Order, Fed. Comm. Comm'n, CC Docket No. 94-102, Dec. 23, 1997.

22 Since cellular telephone companies generally collect telephone numbers and cell site information for internal billing purposes, meeting the requirements of Phase I was viewed as neither difficult nor expensive.

capability of identifying the latitude and longitude of mobile units making 911 calls within a radius of no more than 125 meters. Carriers were to select either a handset-based technology[23] or a network-based technology[24] for this *automatic location information* (ALI) and report their decision to the FCC by November 2000. In their declarations, most of the major carriers indicated that they would use handset-based GPS to meet the mandate,[25] partly because a network-based solution is less accurate and does not work as well in rural areas.[26]

The handset-based location technology—with an integrated GPS receiver and processor built into the handset[27]—requires carriers to ultimately be able to locate callers within 50 meters for 67 percent of calls, and 150 meters for 95 percent of calls.[28] This is not nearly as accurate as full, albeit cost-prohibitive, GPS capability, which could target individuals to within three or four meters. Yet Phase II requirements are expected to afford carriers with a fair amount of location information and tracking ability. The technology can determine not only location, but also where someone is

---

[23] A handset-based solution requires modifications to the handset, such as Advanced Forward Link Triangulation (A-FLT) or Global Positioning System (GPS) capability. The GPS capability can be divided into stand-alone and network-assisted systems. A handset equipped with GPS capability references a constellation of 24 GPS satellites that circle the earth every 12 hours to determine its current position. In a network-assisted GPS system, information from additional ground-based, or terrestrial, transmitters is used to shorten the time to locate and increase the accuracy of the handset position. *See* Overview of ALLTEL's Wireless Network (as submitted to the FCC), http://www.fcc.gov/e911/meetingminutes070600.txt (last visited March 2001)..

[24] A network-based solution is an overlay network where the location sensor resides in the network and additional equipment is installed at the cell site. There are several approaches: Angle of Arrival (AOA), Time Difference of Arrival (TDOA), and Fingerprinting. All of these rely on a signal transmitted from the handset to multiple fixed base stations to determine the position of the handset. *Id.* One of the largest companies solely dedicated to wireless location capability is True Position, whose spokesman describes its network-based system as follows: "True Position collects radio signals at the various cell towers. We put a box about the size of a VCR which is the network overlay, and that is placed right on the cell tower, and it captures that radio signal. And through a triangulation capability, through mathematical algorithms, we basically compute the XY coordinates." Federal Trade Commission, The Wireless Web Workshop, The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues, (Dec. 12, 2000) (statement by Michael Amarosa), *available at* http://www.ftc.gov/bcp/workshops/wireless/001212.htm [hereinafter Workshop]. One major difference between the network and handset solution is that with the network, the brains of the system processing capability physically reside with the network, and with the handset solution, these reside with the handset itself. *See* Workshop, *supra* (statement by Jonas Neihardt).

[25] Workshop, *supra* note 24 (statement by Jonas Neihardt).

[26] *See id.* One panelist commented that with the network-based solution, unless cell sites are arranged in triangles, the triangulation method used may not accurately locate a handset.

[27] *See* 47 C.F.R. § 20.18(h)(2) (2003); *see also* Workshop, *supra* note 24.

[28] In contrast, network-based technology would only need to be accurate to 100 meters for 67 percent of calls, and 300 meters—or about the equivalent of an entire neighborhood—for 95 percent of calls. *See* 47 C.F.R. § 20.18(h)(1); *see also* Workshop, *supra* note 24.

heading and how quickly. Users may also be tracked not only while they are talking, but whenever their phones are turned on.[29]

Phase II requirements were to be completed by October 1, 2001, with carriers beginning to sell and activate ALI-capable handsets.[30] But only one carrier, Sprint, met the handset deadline, and no carrier had produced a workable network system.[31] The FCC reluctantly extended various compliance deadlines to 2003.[32] The FCC still maintains a full implementation deadline of December 31, 2005, when all carriers must ensure that 95 percent of their customers have location-capable handsets.[33]

Unfortunately, while this location information and tracking capability will serve to ultimately help the millions of Americans who call 911 each year,[34] government agents may also be able to quietly access and use this information for other purposes and without limitation. Privacy advocates suggest that police might use location information, for example, to accuse a crash victim of drinking and driving if tracking records indicate the victim had just left a bar.[35] Could such surveillance occur? On the one hand, the FBI is reportedly building a data-mining system that will draw in huge amounts of commercial and governmental information.[36] Since the events of September 11, 2001, many telecommunications carriers have voluntarily turned over customer data to law enforcement agents.[37] Law enforcement demands to intercept and moni-

---

[29] *See* Bouvet, *supra* note 11. This is because a cell phone sends out signals to the service provider every few minutes, whether it is in use or not. This is also a concern as users gravitate toward smart phones with an "always on" Internet connection.

[30] The rules originally required that by December 31, 2001, 25 percent of a carrier's new handset activations must be ALI-capable; 50 percent must be ALI-capable by June 30, 2002; and by December 31, 2002, 100 percent of that carrier's new digital handset activations must be ALI-capable. For any carriers deploying a network-based ALI solution, the carrier must provide Phase II service to 50 percent of callers within six months of a PSAP request and up to 100 percent of callers within 18 months of the PSAP request. *See* Public Notice, *Wireless Telecommunications Bureau Provides Guidance on Carrier Reports on Implementation of Wireless E911 Phase II Automatic Location Identification*, Fed. Comm. Comm'n, CC Docket No. 94-102, http://www.fcc.gov/Bureaus/Wireless/Public_Notices/2000/da002099.html (Sept. 14, 2000).

[31] *See* Ben Charny, *Carriers Win E911 Delays*, CNET, *at* http://news.com.com/2100-1033-273995.html (Oct. 5, 2001). Carriers such as Nextel Communications, however, were expected to begin selling location-capable phones by the end of 2002. *Id.*

[32] *See* In the Matter of Revision, Order to Stay, *supra* note 3. The FCC extended its E911 Phase II interim handset and network upgrade compliance deadlines by seven months for Tier II carriers and by thirteen months for Tier III carriers.

[33] *See id.*

[34] In 2000, approximately 45 million emergency 911 calls were received from wireless phones. *See* Schwartz, *supra* note 13.

[35] *See* Sevitt, *supra* note 10.

[36] *See* Robert O'Harrow, Jr., *Six Weeks in Autumn*, WASH. POST, Oct. 22, 2002, http://www.washingtonpost.com/wp-dyn/articles/A1999-2002Oct22.html.

[37] *See* Jane Black, *Uncle Sam Needs Watching, Too*, BUS.WK., Nov. 30, 2001, *available at* http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011129_3806.htm.

tor electronic communications have also increased, with the total number of wiretaps in 2001 jumping 25 percent from the previous year, and roughly two-thirds conducted on portable devices such as pagers and cell phones.[38] The likelihood of a wiretapping is expected to rise tenfold,[39] and one recent report estimates that local police illegally underreport wiretaps by a factor of ten.[40] Federal government surveillance records are often kept secret,[41] but stories about misuse are starting to surface.[42]

The wiretap threat to wireless devices such as cellular phones is of particular concern. Privacy is especially fragile with cell phones because these devices are more closely associated with the individual owner. Call location information can be tracked over time and stored, leading to the creation of very detailed personal information.[43] The vast majority of cell phone users (81 percent) say it is "extremely important" that they be able to turn location tracking off,[44] yet even if this were technically possible from a commercial standpoint, the government may be able to easily demand that tracking be made available for law enforcement purposes.

The extent to which law enforcement agencies are permitted to follow the electronic footprints under existing law is not known. How call location privacy interests will be treated by the courts or under current statutory law is unclear. The following section explores location privacy rights under Fourth Amendment jurisprudence. Then various statutory laws and their application to call location information are examined.

II. LOCATION PRIVACY RIGHTS UNDER THE U.S. CONSTITUTION

Government monitoring and tracking of call location information may invoke a constitutional right of privacy found within the

---

38 *See* Declan McCullagh, *Busy Year for Big Brother*, WIRED NEWS, *at* http://www.wired.com/news/politics/0,1283,52781,00.html (May 25, 2002).

39 *See* Black, *supra* note 37.

40 *See* McCullagh, *supra* note 38.

41 Because of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (amending scattered sections of 18, 47, 50 U.S.C.) [hereinafter USA Patriot Act of 2001]), wiretaps may be more easily authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA), which permits a secret proceeding by a secret FISA court that only looks to see that certifications are present and not "clearly erroneous." Rachel King, *Q: Is Congress Giving Too Much Surveillance Power To Federal Law Enforcement?*, INSIGHT ON THE NEWS, Jan. 14, 2002, at 40, *available at* LEXIS, News Library. The orders are never open to the public, and because FISA does not require notice to be given to a target, the subject of the order never knows that the government was spying on him. *See* King, *supra.*

42 *See* Noelle Straub, *USA Patriot Act Powers Prompt Second Look*, THE HILL, May 1, 2002, http://www.hillnews.com/050102/patriot.shtm.

43 *See* Newcombe, *supra* note 6.

44 *See Your Phone Knows*, *supra* note 2.

Fourth Amendment,[45] although this protection may be extremely limited at best. While surveillance and disclosure of such information by private entities is outside the scope of constitutional protection, unreasonable searches and seizures by the government fall under Fourth Amendment jurisprudence.[46] The Fourth Amendment provides that the "right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated. . . ."[47] No case law specifically addresses a constitutional right to call location privacy, although constitutional protection has been claimed in some similar cases dealing with electronic surveillance, such as the monitoring and recording of telephone calls and the use of electronic tracking beepers. Courts, in determining a right of location privacy, will likely rely on these precedents. Yet in most of these cases, the Supreme Court and lower courts have ruled in favor of the government.

A. *Telephone Monitoring*

In the landmark privacy case *Katz v. United States*,[48] the Supreme Court essentially established that the Fourth Amendment protects the contents of a traditional telephone call. Until this 1967 case, constitutional protection did not pertain unless the government physically searched or seized tangible property.[49] With *Katz*, however, the High Court stated that "the Fourth Amendment protects people, not places,"[50] and subsequently created an "expectation of privacy" standard for determining infringement. The standard essentially asks whether the individual, by his or her conduct, has "exhibited an actual (subjective) expectation of privacy,"[51] having shown that he or she "seeks to preserve

---

45 Although a right of privacy is not explicitly stated in the U.S. Constitution, it has an implicit textual basis found in several amendments such as the Fourth Amendment. *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

46 The search and seizure clause of the U.S. Constitution does not protect citizens from unreasonable searches by private parties. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 113-14 (1984); Jackson v. Metropolitan Edison Co., 419 U.S. 345, 349 (1974).

47 U.S. CONST. amend. IV.

48 389 U.S. 347 (1967).

49 *See* Olmstead v. United States, 277 U.S. 438 (1928). In 1928, the Supreme Court reasoned that warrantless wiretapping of a phone by government officials did not violate the provisions of the Fourth Amendment because wiretapping did not involve physical intrusion into one's home. In the now famous dissent, Justice Brandeis wrote that the Founders of the Constitution "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." *Id.*. at 478 (Brandeis, J., dissenting).

50 *Katz*, 389 U.S. at 351.

51 *Id.* at 361.

(something) as private."[52] The analysis then asks whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[53] In *Katz*, FBI agents acting without a warrant attached a listening device to the outside of a public phone booth to monitor the defendant's conversation.[54] The Court found the practice to be an unconstitutional search and seizure, essentially concluding that *Katz* had an expectation of privacy in the contents of a telephone call.

Yet while call location information might therefore seem protected under *Katz*, this high level of protection does not necessarily apply to call characteristics beyond the oral contents.[55] In 1979, the Supreme Court employed the *Katz* analysis in *Smith v. Maryland*,[56] deciding that the utilization of a pen register, which records the numbers dialed from a telephone,[57] did not constitute a search or necessitate a warrant under the U.S. Constitution. In this case, where the telephone company used a pen register at police request to record the numbers dialed from the home of a man suspected of placing threatening calls to a robbery victim, the Court found there was no "expectation of privacy" in the numbers a person dials.[58]

> [W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through the telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list

---

52 *Id.* at 351.

53 *Id.* at 361. Most adjudication has relied on the second part of the inquiry, which remains the prevailing authority. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974).

54 *See Katz*, 389 U.S. at 348.

55 Many lower courts have held that an expectation of privacy protected under the Fourth Amendment only extends to the content of telephone conversations and not to the records or the fact that conversations took place. *See, e.g.*, Nolan v. United States, 423 F.2d 1031 (10th Cir. 1969); United States v. Baxter, 492 F.2d 150 (9th Cir. 1973); United States v. Lustig, 555 F.2d 737 (9th Cir. 1977); Indiana Bell Tel. Co. v. State of Indiana (*In re* Order for Indiana Bell Tel. to Disclose Records), 409 N.E.2d 1089 (Ind. 1980); Hadley v. State, 735 S.W.2d 522 (Tex. Ct. App. 1987).

56 442 U.S. 735 (1979).

57 A pen register is a mechanical device, usually installed by the telephone company at the central office, that can decode and record the numbers dialed from a particular telephone. Local exchange carriers typically use pen registers to monitor equipment and facilities or identify the source of obscene or abusive calls. A trap and trace device (sometimes known as a cross frame unit, card drop, and touch-tone decoder) captures electronic impulses that identify the originating number of an incoming wire or electronic communication. Neither device enables anyone to hear or record the content of the communication.

58 *See Smith*, 442 U.S. at 742.

of their long distance (toll) calls on their monthly bills.[59]

The Court stated that people also realize that devices are used for the purpose of checking billing operations, detecting fraud, and preventing violations of law such as obscene phone calls.[60] The Court was not persuaded by arguments that numbers dialed "reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[61] Moreover, the Court found that even though the caller in this case may have intentionally called from the privacy of his home in order to keep the *contents* of his conversation private, his *conduct* (placing the call) was not calculated to preserve the number he dialed.[62]

In applying the second part of the *Katz* test, the Court stated that even if an expectation of privacy existed, it was not one that society would recognize as reasonable.[63] The Court stated that when the petitioner used the phone, he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In doing so, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[64]

As a result of *Smith*, wireless call location information would seemingly be denied Fourth Amendment protection. Many courts have since invoked *Smith*,[65] with some even finding no expectation of privacy in telephone company records identifying the name or address of a subscriber.[66] Courts, in turn, may easily conclude that call location information is analogous to information associated with the numbers dialed. In both cases, the information is associated with the conduct of the call and not the contents. Telephone users are also aware that location information is collected by the service provider for normal business purposes in order to complete the connection, assess roaming charges, and now forward E911

---

59 *Id.*

60 *See id.*

61 *See id.* at 748 (Steward, J. dissenting).

62 *See id.* at 743.

63 *Id.*

64 *Id.* at 743-44.

65 *See, e.g.*, Yarbrough v. State, 473 So. 2d 766 (Fla. 1985); United States v. Mosko, 654 F. Supp. 402 (D. Colo 1987).

66 *See, e.g.*, United States v. Ahumada-Avalos, 875 F. 2d 661 (9th Cir. 1989). Many other courts have found no expectation of privacy in telephone toll records. *See* United States v. Doe, 537 F. Supp. 838 (E.D.N.Y. 1982); United States v. X, 601 F. Supp. 1039 (D. Md. 1984); Kesler v. State, 291 S.E.2d 497 (Ga. 1982); Indiana Nat. Bank v. Chapman, 482 N.E.2d 474 (Ind. Ct. App. 1985); Hadley v. State, 735 S.W.2d 522 (Tex. Ct. App. 1987); Indiana Bell Tel. Co. v. State of Indiana (*In re* Order for Indiana Bell Tel. to Disclose Records), 409 N.E.2d 1089 (Ind. 1980); United States v. Grabow, 621 F. Supp. 787 (D. Colo. 1985); State v. Hamzy, 709 S.W.2d 397 (Ark. 1986).

calls to emergency service providers. With ever-increasing awareness of these capabilities, it would seemingly be difficult for an individual to claim an expectation of privacy in call location information that identifies the cell site in use or perhaps even one's physical location through triangulation or other means. Even so, courts may conclude that any such expectation of privacy is not one that society is willing to accept as reasonable. Since *Smith*, courts have repeatedly said that by revealing their affairs to third parties (i.e., the telephone company), subscribers take a risk that the information will be conveyed to law enforcement officials.[67] Call location information is voluntarily disclosed to the telephone company by callers who could arguably find alternative means of communication in order to preserve their privacy.

B. *Electronic Tracking Beepers*

Another form of government surveillance that may be found analogous to call location monitoring and hence give rise to Fourth Amendment scrutiny is the use of electronic tracking beepers.[68] These small devices, which can be surreptitiously attached and emit a signal receivable up to several miles, are sometimes used by law enforcement agencies to track the location of suspicious criminals' cars or belongings in transit. Because location information is the objective of tracking beepers, precedent associated with their use may be even more applicable than for pen registers and trap and trace devices. Here the protection may be limited, though, depending on where the tracking takes place.

The definitive case is *United States v. Knotts*,[69] in which the Supreme Court, applying the two-part *Katz* test, found no expectation of privacy in the information obtained from an electronic tracking beeper. In *Knotts*, police had a beeper attached to a container of chemicals that they then tracked across two states to a cabin occupied by the respondent who was subsequently convicted of conspir-

---

[67] It is of interest to note that in *Smith*, and other cases, the telephone company was considered a *third party* to whom the subscriber risked conveying information. In most cases, the telephone company provided the information at the request of the government. However, if a third party *voluntarily*, and not acting as an agent for the government, conveys confidential information to law enforcement officials, Fourth Amendment privacy rights are not applicable. *See* S.E.C. v. O'Brien, Inc., 467 U.S. 735 (1984).

[68] A distinction must be made here between the use of electronic tracking beepers and their installation. A number of lower courts have found that the installation of such beepers without a warrant violates the Fourth Amendment. *See* Richard H. McAdams, *Tying Privacy in Knotts: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297 (1985). Since call location tracking does not involve any installation of a device, an analysis of only the use of tracking is at issue here.

[69] 460 U.S. 276 (1983).

acy to manufacture controlled substances. Although police had obtained a search warrant for the cabin, Knotts argued that the use of the tracking beeper required a warrant. The Supreme Court did not agree, pointing to the fact that the police had used the beeper along "public streets and highways."[70] The Court reasoned "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[71] Such information could be obtained by anyone through traditional means—such as physically following and watching the suspect. The fact that an electronic device was employed was irrelevant. The Court concluded "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them."[72]

Given that cellular phones and other wireless devices are typically used on streets and other public places, this same reasoning could apply to call location tracking. Courts could simply find that using call location technology is merely an "enhancement" to law enforcement's ability to otherwise visually follow wireless phone users. Any argument that such monitoring could easily get out of hand may also be unpersuasive. The Court in *Knotts* rejected the argument that if permitted, police would engage in widespread monitoring, stating that the "reality hardly suggests abuse."[73] The Court did, however, remain open to the possibility that "dragnet type law enforcement practices"[74] may someday occur, but concluded that there would be "time enough then to determine whether different constitutional principles may be applicable."[75] In this sense, pervasive tracking and hence abuse of call location information may also have to occur before Fourth Amendment protection may apply to call location monitoring. Unfortunately, since notification and reporting may not be required,[76] the extent to which tracking is done may never be known.

---

70 *Id.* at 279.

71 *Id.* at 281. The Court also noted the generally diminished expectation of privacy inside automobiles.

72 *Id.* at 282.

73 *Id.* at 283 (quoting Zureter v. Stanford Daily, 436 U.S. 547, 566 (1978)).

74 *Id.* at 284.

75 *Id.*

76 While it does not address location information specifically, the USA Patriot Act of 2001, for example, eliminates the notification and reporting requirements when it comes to government searches and seizures of phone company business records. *See* King, *supra* note 41; *EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities*, Electronic Frontier Foundation, *at* http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php (Oct. 31, 2001) [hereinafter *EFF Analysis*].

The location of the tracking may nevertheless be a key factor, as distinguished by the Supreme Court one year later in *United States v. Karo*.[77] Here, a beeper was attached to a container of drug manufacturing chemicals in order to determine whether the container was inside a certain private residence. Because information obtained about the inside of the residence could not have otherwise been ascertained by the naked eye, the Court held that the use of an electronic tracking device amounted to an illegal search. The Court stated "[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."[78]

Thus, the home may be protected from tracking. Indeed, the High Court has long recognized that the Fourth Amendment draws a firm line at the entrance of the home.[79] Of course this protection is not absolute. Subsequent decisions, for example, indicate that aerial surveillance of private homes and surrounding areas does not necessarily constitute a search if there is no expectation of privacy that society is willing to recognize as reasonable.[80] Yet in a recent case, *Kyllo v. United States*,[81] the Supreme Court limited how much technological enhancement may be employed in home surveillance. In finding thermal imaging of a residence unconstitutional, the Court distinguished thermal imaging as something that is not in general public use and that can explore details of a home that are unknowable without a physical search.

Because of *Karo* and *Kyllo*, call location information may therefore receive some protection if law enforcement has to limit call location surveillance to only cell sites or approximate locations and away from homes. Yet these rulings might not prohibit the ability to track location *to* a private residence necessarily; rather the police may only be precluded from using the information to point to specific locations *within* a residence. How this might limit monitoring of semi-private locations such as hotels and office buildings is not clear.

Thus, from pen registers and trap and trace devices to electronic tracking devices, the applicable legal precedents for call location information do not present much hope for Fourth

---

77 468 U.S. 705 (1984).

78 *Id.* at 716.

79 *See* Payton v. New York, 445 U.S. 573, 590 (1980).

80 *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986); Florida v. Riley, 488 U.S. 445 (1989).

81 533 U.S. 27 (2001).

Amendment protection. Until courts specifically address the issue, the warrantless use of call location information technology by the government may not rise to the level of an unconstitutional search and seizure. Unless legal limitations pertaining to private locations are recognized as in *Karo* and *Kyllo,* or widespread police monitoring is discovered, prompting public outcry and judicial review, police may engage in unrestrained, surreptitious monitoring of call location information. As a result, legislative guidance is needed.

III. Location Privacy Rights Under Federal Statutory Law

Several federal statutory laws may extend protection to wireless location information, although the extent of this protection from unauthorized government tracking is similarly unclear. The Omnibus Crime Control and Safe Streets Act of 1968[82] (Title III) was created with the explicit purpose of balancing the legitimate needs of law enforcement with the public's need for privacy. The Electronic Communications Privacy Act of 1986[83] (ECPA) further extends these protections for wire and oral communications to new electronic communications such as cellular telephones and email. In 1994, the Communications Assistance for Law Enforcement Act[84] (CALEA) was created to ensure that law enforcement officials were able to conduct electronic surveillance in the face of rapidly changing telecommunications technology, while still recognizing privacy rights. Yet in 2001, the Patriot Act[85] further expanded law enforcement authority over electronic surveillance, permitting easier access to telecommunication subscriber records and wiretapping.[86] The result is a compilation of laws that provide limited privacy protection for wireless communications. Which, if any, protections pertain to call location information is uncertain.

A. *Title III and the ECPA*

1. Tracking

Some of the confusion rests with how call location information is defined. If it is considered to be tracking information, the ECPA may exclude it from the privacy protections generally afforded other communications technologies. The ECPA grants certain

---

82 18 U.S.C. §§ 2510-2520 (1970 & Supp. 1996).

83 Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (1988)).

84 Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in 18 U.S.C. § 2522 (1994), and 47 U.S.C. §§ 1001-1010 (1994)).

85 *See supra* note 41.

86 *See EFF Analysis, supra* note 76.

protections to *electronic communications*, as defined in Section 2510(12). But subsection C explicitly excludes from this definition "any communication from a tracking device."[87] Thus, while the ECPA covers cellular phone use, the tracking of cell phone calls may fall outside the scope of this part of the law. Further interpretation is needed.

Another section of the Act does, however, address *mobile tracking devices*,[88] which may be construed as similar in objective to call location tracking. A mobile tracking device is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[89] While this generally means a tracking beeper attached to a moving car or object,[90] it is possible that call location tracking from a telephone company or Internet Service Provider may apply. Again, further interpretation is needed. Unfortunately, if this section is found to apply, the law does not afford any clear guidance or protection. The law only addresses jurisdictional aspects and only "if a court is empowered to issue a warrant or other order for the installation of a mobile tracking device."[91] No part of this law or other law explains how this authorization may be given or what level of court order is required.[92] In addition to this potentially weak authorization, the law allows considerable latitude in where such devices may be used. A court may authorize the use of a tracking device not only within its area of jurisdiction, but also "outside that jurisdiction if the device is installed in that jurisdiction."[93] Thus, nationwide jurisdiction is effectively possible, making it easier for law enforcement to engage in surveillance and more difficult for targets to contest a court

---

87 This is because electronic tracking devices do not intercept the content of communications within the meaning of 18 U.S.C. § 2510.

88 *See* 18 U.S.C. § 3117.

89 *Id.* § (b).

90 *See, e.g.*, United States v. Rowland, 145 F.3d 1194 (10th Cir. 1998).

91 18 U.S.C. § 3117(a).

92 In a case scrutinizing court authority, the U.S. District Court for the District of Massachusetts pointed to this flaw in the law. *See* United States v. *In Re:* Application of the United States For an Order Authorizing the Installation, Monitoring, Maintaining, Repairing, and Removing of Electronic Transmitting Devices ("Beepers") and Infra-Red Tracking Devices On or Within a White Ford Truck VIN 1FDKE37HHB79229, No. 94-M0019-01-LPC, 155 F.R.D. 401 (D.MA. Apr. 8, 1994). The court stated that "[a]t first blush, . . .one might conclude that Section 3117 is applicable by its very terms if, and only if, a judge or magistrate judge is otherwise 'empowered to issue a warrant or other order for the installation of a mobile tracking device.' That is to say, a natural reading of that language may suggest that one must look elsewhere to positive law - i.e., a codified statute or rule - to determine whether that authority exists. And therein, of course, lies the rub, since there is no positive law, statute or rule, which grants such authorization." *Id.* at 402.

93 18 U.S.C. § 3117(a).

order.[94]

2. Pen Registers/Trap And Trace Devices

Call location information may instead find protection under provisions pertaining to pen registers and trap and trace devices.[95] Since *Katz*, pen registers and trap and trace devices have been given certain statutory privacy protections that limit government surveillance of traditional wireline communications.[96] These provisions could be interpreted as extending to wireless call identification information, which could further extend to location information. By definition, though, these provisions may not apply because pen registers and trap and trace devices are specifically defined as capturing the telephone "numbers dialed or otherwise transmitted. . . ."[97]—which does not explicitly include such call identifying information as geographic location. The 2001 Patriot Act, however, recently amended the law to extend government surveillance authority over pen registers and trap and trace devices to the Internet and other computer networks.[98] Now, officials may collect information such as web site addresses, Internet protocol addresses, port numbers, and similar computer addresses. Still, these changes do not specify wireless geographic location information.

Yet even if these provisions are found to apply, the current protection against the use of pen registers and trap and trace devices is not as strong as for other forms of wiretapping because the content of the communication is not intercepted. Government officials must apply for a court order,[99] but the application falls far short of a search warrant required for access to call content. For other wiretap applications under Title III, law enforcement must show several things, including probable cause that a person is committing, has committed, or is about to commit a crime.[100] In con-

---

94 This law also does not bar use of evidence acquired without a § 3117 order. *See* United States v. Gbemisola 225 F.3d 753 (D.C. Cir. 2000).

95 18 U.S.C. §§ 3121-3127 (1986).

96 *See id. See, e.g.*, § 3121(a) (prohibiting any person, including law enforcement, from installing or using a pen register or a trap and trace device without first obtaining a court order).

97 A pen register is defined as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached. . . ." 18 U.S.C. § 3127(3). A trap and trace device is defined as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communications was transmitted. . . ." 18 U.S.C. § 3127(4).

98 *See* USA Patriot Act of 2001 § 216 (amending 18 U.S.C. §§ 3121, 3123, 3124, 3127).

99 18 U.S.C. § 3121(a).

100 18 U.S.C. § 2518(3)(a) (1968).

trast, applications for pen registers and trap and trace devices only require the government to certify that the information to be obtained is "relevant to an ongoing criminal investigation."[101] How directly one must be associated with such an "investigation" is an issue, since law enforcement agents only have to prove that the information sought—not the individual—is relevant to an investigation.[102] The 2001 Patriot Act further erodes the level of proof by permitting law enforcement agents to evade the probable cause requirement and conduct surreptitious wiretaps, including roving wiretaps,[103] by relying on the looser standards of the Foreign Intelligence Surveillance Act of 1978 (FISA).[104]

Pen register and trap and trace authority is also problematic in that orders are generally rubberstamped without question.[105] The orders may also be valid for sixty days[106] and can be extended,[107] while other wiretap orders are good for only up to 30 days.[108] And while the law requires that an order specify the location of the telephone line to be tapped, it is only required if *known.*[109] Thus, if government requests for location information are considered analogous to pen registers and trap and trace devices, very little scrutiny and judicial oversight may occur. If the government does not need to show probable cause of a crime, communications networks could end up entertaining a flood of long-term requests to monitor callers who may never be connected to criminal activity.

3. Stored Wire And Electronic Communications

Another source of statutory protection for location information may be found in the Stored Wire and Electronic Communica-

---

101 18 U.S.C. § 3123(a).

102 *See* Chris Oakes, *'E911' Turns Cell Phones into Tracking Devices*, WIRED NEWS, *at* http://www.wired.com/news/technology/0,1282,9502,00.html (Jan. 6, 1998). This presents the additional problem of innocent bystanders being tracked if, for example, they are in the same car as the target. *See* Newcombe, *supra* note 6.

103 *See* USA Patriot Act of 2001 § 206 (amending 50 U.S.C. § 1805(c)(2)(B)(1978)). A roving wiretap enables government investigators to intercept all of a suspect's wire or electronic communications related to conduct that is under investigation, regardless of the suspect's location. It essentially allows law enforcement to follow a suspected criminal from one phone to another without getting a new warrant whenever the target switches lines to purposefully or effectively thwart a tap.

104 *See EFF Analysis, supra* note 76.

105 Attorney Michael Gross states that "[t]he judges appointed in recent years have a tendency to assume and rely upon an assumption that the government wouldn't be asking if they weren't entitled. They don't put the applicant through as severe a test for proof as they used to." Schwartz, *supra* note 13.

106 *See* 18 U.S.C. § 3123(c)(1).

107 *See id.* § (c)(2).

108 *See* 18 U.S.C. § 2518(5).

109 *See* USA Patriot Act of 2001 §§ 216 (amending 18 U.S.C. 3123(b)(1)(C)), 214 (amending 50 U.S.C. 1842(d)(2)(A)(iii)(1978)).

tions provisions of the ECPA.[110] These provisions govern the government's ability to require a provider of electronic communication service or remote computing service to disclose "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber. . . ."[111] While these provisions do not specifically mention location information, the Department of Justice has determined that certain location information—at least in the context of 911 calls—is covered.[112] In a memorandum opinion on the legality of the FCC's E911 requirements, the Department of Justice (DOJ) stated that section 2703 of the ECPA applies to a cellular service carrier's transmission of location information to 911 operators.[113] The DOJ further concluded that the E911 rules do not violate Title III, the ECPA, or the Fourth Amendment because a caller dialing 911 has "impliedly consented to such disclosure, thus permitting the Federal Government to require the carrier to disclose such [location] information without a warrant or Court order."[114] The DOJ stated that a 911 caller has "neither an actual nor a reasonable expectation of privacy with regard to his or her whereabouts at the time of the call."[115]

This interpretation could possibly carry over to all types of location information, not just that associated with 911. At least under section 2703 and as with pen registers and trap and trace devices, law enforcement agencies generally must obtain a court order before gaining access to the information.[116] Yet likewise, this protection is not strong when such a court order falls short of a probable cause showing required by a search warrant. Even more frustrating is the conclusion of the Justice Department that in the case of 911 calls, the caller has impliedly consented to such a disclosure, thus possibly permitting the government to require the carrier to disclose the information *without* a warrant or court order.[117] As a result, in this context, there could be even less protec-

---

110 *See* 18 U.S.C. § 2703.

111 *Id.* § (c)(1)(C).

112 *See* Memorandum Opinion Issued by Department of Justice Concludes that Commission's Recently Adopted Wireless Enhanced 911 Rules are Consistent with Wiretap Act, Fed. Comm. Comm'n, CC Docket No. 94-102, Dec. 10, 1996, http://ftp.fcc.gov/Bureaus/Common_Carrier/Public_Notices/1996/da962067.txt [hereinafter Memorandum Opinion].

113 *See id.*

114 *Id.*

115 *Id.*

116 *See* 18 U.S.C. § 2703(c)(1)(B)(ii). Government entities may also access this information with a warrant or with consent of the subscriber or customer. *See id.* §§ 2703(c)(1)(B)(i), (iii).

117 *See* Memorandum Opinion, *supra* note 112.

tion for call location information.

B. *CALEA*

Location information is specifically mentioned in the Communications Assistance for Law Enforcement Act of 1994 (CALEA), which would seem to be the most applicable legislation yet. This Act requires a telecommunications carrier to ensure that its equipment, facilities, or services are capable of enabling the government to intercept all electronic communications carried by the carrier—including "call-identifying information," before, during, or after transmission.[118] Call-identifying information is defined as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber. . . ."[119] Yet while this would seem to describe location information, the law specifically states that except with regard to information obtained by 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 (except to the extent that the location may be determined by the telephone number). . . ." (emphasis added).[120] Thus under CALEA, location information is distinguished and appears to be specifically protected.

Yet this protection under CALEA is still up in the air, since CALEA requires the Federal Communications Commission to create rules,[121] and the FCC in 1999 adopted standards that nonetheless require location information be available to law enforcement agencies (LEAs).[122] The FCC determined that "call-identifying information" such as the "origin" or "destination" of a communication essentially means location information.[123] Therefore, according to the FCC, location information would have to be made available to law enforcement under CALEA. Carriers would not have to provide the precise *physical* location of a caller, though,

---

118 *See* 47 U.S.C. § 1002(a)(2)(A) (1994).

119 *Id.* § 1001(2).

120 *Id.* § 1002(a)(2)(B). CALEA, which strives to balance law enforcement needs with privacy, also requires telecommunications providers to protect the privacy and security of call-identifying information that is not authorized to be intercepted, and to otherwise ensure that any interception is activated with a court order or other lawful authorization. *See* 47 U.S.C. §§ 1002(a)(4)(A), 1004.

121 47 U.S.C. § 229(a) (1934).

122 *See In re* Communications Assistance for Law Enforcement Act, Third Report and Order, 14 F.C.C.R. 16794, 16815 (Fed. Comm. Comm'n 1999) [hereinafter Third Report and Order].

123 *Id.* at 16813.

thus satisfying the exclusion requirement stipulated by CALEA.[124] Rather, the FCC standards would permit legally authorized LEAs to receive only the location of a cell site at the beginning and end of a mobile call.[125]

As a result, privacy advocates have complained that the FCC is threatening civil liberties, potentially granting the FBI new powers of surveillance.[126] The American Civil Liberties Union, the Electronic Privacy Information Center, and the Electronic Frontier Foundation have argued that CALEA contains no provisions expressly including location-tracking data within the definition of call-identifying information.[127] The Center for Democracy and Technology has argued that the words "origin" and "destination" have meanings apart from location, and that the location of wireless phones is more personally revealing than the location of wireline phones because wireless calls are always made by individual subscribers.[128] Unconvinced, the FCC has concluded that the wireless location information associated with cell site location is equivalent to location information associated with wireline phones; therefore, providing this information is within the law.[129]

Several privacy organizations asked the U.S. Court of Appeals in 2000 to suspend the rules, complaining, in part, that the rules do not require police to obtain a search warrant.[130] As with pen registers and trap and trace devices, CALEA only requires the government to get a court order, or at minimum, any "other lawful authorization."[131] Making matters more complicated, the FCC only requires LEAs to obtain "authorization different from the minimal authorization necessary for use of pen registers and trap and devices."[132] No explanation is given for what this "different" authorization might be. The FCC has also stated that while it did

---

124 The FCC, in fact, rejected a New York Police Department proposal that would have required triangulating signals from multiple cellular antenna towers to pinpoint a wireless phone's precise location throughout a call's duration. *Id.* at 16815-16. The FBI had also sought legislation that would give it easier access to the precise physical location of cell phone users. FBI Director Louis Freeh asked the Senate Appropriations Committee to require cellular phone location information without a court order in certain emergencies. *See* Oakes, *supra* note 14.

125 *See* Third Report and Order, *supra* note 122, at 16815.

126 *See* James Glave, *FCC Sides with FBI on Tapping*, WIRED NEWS, *at* http://www.wired.com/news/politics/0,1283,21477,00.html (Aug. 27, 1999).

127 *See* Third Report and Order, *supra* note 122, at 16814.

128 *See id.* at 16813.

129 *See id.* at 16816.

130 *See* William Mathews, *Privacy Advocates Challenge FBI Cell Phone Tracking*, FED. COMPUTER WK., *at* http://www.fcw.com/fcw/articles/2000/0124/web-privacy-01-24-00.asp (Jan. 24, 2000).

131 47 U.S.C. § 1002(a)(2).

132 Third Report and Order, *supra* note 122, at 16813.

not mandate full location tracking capabilities, its decision "does not preclude LEAs from requesting legal authority to acquire more specific location information in particular circumstances."[133] The appeals court in *United States Telecom Ass'n v. FCC*[134] affirmed this portion of the FCC's decision pertaining to location information, acknowledging the "different" authorization prescribed by the FCC.[135] Yet like the FCC, the federal court offered no further explanation, leaving legal experts to wonder if a slightly higher standard may have been created.[136] Further clarification is needed.

C. *Wireless Communications and Public Safety Act of 1999*

Finally, another statutory provision that may pertain to call location information is the Wireless Communications and Public Safety Act of 1999,[137] which directs the FCC to designate 911 as the universal emergency telephone number. This law applies to both wireline and wireless telephone service and authorizes telecommunications carriers to provide call location information to a public safety answering point (PSAP), other emergency service provider, or to other data base providers solely for assisting in the delivery of emergency services.[138] The law also permits the release of location information to the user's immediate family in the case of serious physical harm.[139] For disclosure of call location information and automatic crash notification information to any other person, a customer's express prior authorization is required.[140] The law does not specifically address government access, however, leaving the level of authorization required for LEAs uncertain.

IV. SUGGESTIONS AND CONCLUSIONS

Current law thus provides little, if any, clear protection for wireless call location information. Constitutional protection may not be invoked partly because the actual contents of a communica-

---

133 *Id.* at 16816.

134 227 F.3d 450 (D.C. Cir. 2000).

135 *Id.* The appeals court did, however, create more protection for packet-mode communications in the event that it is difficult to separate the call-identifying information from call content. In this case, because content may be accessed, a search warrant is required. This level of authorization was not required of call location information. Yet it is worth noting that in the case of any wireless web communication where content cannot be separated, a request for call location information would therefore require a search warrant.

136 *See* Oscar Cisneros, *FCC Wiretap Order Overturned*, WIRED NEWS, *at* http://www.wired.com/news/print/0,1294,38258,99.html (Aug. 17, 2000).

137 Pub. L. 106-81, 113 Stat. 1286 (1999) (amending 47 U.S.C. §§ 222, 251, and appearing in part as 47 U.S.C. §§ 615, 615 note, 615a, 615b).

138 *Id.* (amending 47 U.S.C. § 222).

139 *See id.*

140 *See id.*

tion are not seized. Courts will also likely find that wireless users have no expectation of privacy in location information that they voluntarily disclose to service providers whom they generally understand collect such information in the ordinary course of business. Presuming most location tracking does not extend inside private residences, the technology used may be seen as merely an enhancement to traditional visual surveillance techniques. Protection may not be granted unless a petitioner can successfully show that the location information is uniquely private, there were no reasonable communication alternatives to preserve his or her privacy, and/or the practice of unwarranted searches has led to such widespread abuse, amounting to an expectation of privacy that society would find reasonable.

Current statutory law is also not clear in how it might protect call location information. Call location information is not defined, possibly excluding it from the weak protections afforded pen registers and trap and trace devices, or worse yet, excluding it from any protection at all if it is ultimately associated with permissible tracking. Even if it is defined as call-identifying information, government applicants for a court order do not need to show probable cause of a crime in order to acquire location information. And while CALEA actually increases protection by preventing the release of *physical* location information, the FCC still permits law enforcement to obtain cell site location information at the beginning and ending of each call and by acquiring authorization that is only somehow "different" from that required for pen registers. As for provisions requiring the release of location information for 911 purposes, law enforcement requests are not specifically addressed and are quite likely to require less than a showing of probable cause.

A. *Potential Legislative Solutions*

The federal court system should not wait until widespread abuse is discovered before reassessing privacy expectations associated with tracking and specifically call location information. But until the courts are presented with a Fourth Amendment call location privacy case, it will be up to Congress and the FCC to afford protection before the technology to track calls becomes pervasive and potentially misused without public knowledge and oversight. Although law enforcement needs enhanced technologies to track and catch criminal activity in an ever-increasingly complex technological society, a balance must be sought to protect individual pri-

vacy. Uniform protection across the states is necessary.[141] Clarifying and amending the existing statutory law is essential.

Congress should consider enacting a new set of laws under some type of "Wireless Call Location Protection Act" to address these amendments and establish rights in location privacy. First, any new law should include location information in the definition of electronic communications (section 2510(12)) to, at minimum, place it within existing law protecting pen registers, trap and trace devices, and stored electronic communications. Second, the law should carefully distinguish call location information from other forms of tracking, amending section 2510(12)(c) so that unlike other forms of tracking, call location information is not excluded from protection. Third, all location information must be protected under CALEA, not just physical location. In this sense, call location information must be distinguished from other call-identifying information. Fourth, 911 statutory provisions, which require the disclosure of call location information to emergency medical providers, should explicitly limit government access to that information. Finally, and of utmost importance, the law must bolster the weak court order requirements under section 3123(a) and CALEA, which only require the government to certify that the information to be obtained is "relevant to an ongoing criminal investigation." Instead, probable cause must be shown that the individual (and not just the information) is directly involved in criminal activity. Judges must therefore exact greater scrutiny when evaluating law enforcement applications to seize call location information.

Some legislative effort has indeed been made toward addressing these concerns, but with no success. Rumblings by privacy advocates prompted the creation of a federal bill in 2000 that would have heightened the standard for location information. Called the Electronic Communications Privacy Act of 2000,[142] H.R. 5018 would have amended sections of the Stored Wire and Electronic Communications provisions of the current law[143] by increasing the standard for a court order before a mobile electronic service could disclose a subscriber's physical location.[144] Such a court order

---

141 In 2001, eight states had introduced legislation affecting wireless communications and privacy of information. A national standard is necessary since location privacy is an interstate issue. *See* Newcombe, *supra* note 6.

142 H.R. 5018, 106th Cong. (2000) (introduced by Rep. Charles T. Canady (R-Fla)) (amending 18 U.S.C. § 2703).

143 *See supra* note 110.

144 The bill would have similarly increased the standard for pen registers and trap and trace devices. H.R. 5018. A similar bill was proposed in the second session called the Digi-

could only be issued if there was "probable cause to believe that (A) an individual is committing, has committed, or is about to commit a felony offense; and (B) the location information sought to be obtained concerns the location of the person believed to have committed, be committing, or be about to commit that offense or a victim of that offense."[145] This proposed law distinguished wireless location information, required a showing of probable cause, and required the order to be relevant to the individual tracked. It also neatly defined when disclosures would be permitted without a court order. As with 911 information, call location information could be provided to emergency medical service providers, to immediate family members in an emergency situation, and with the express consent of the subscriber or user of the equipment.

While the bill would have corrected some of the current statutory deficiencies, it still, however, left somewhat vague the degree to which an individual may be "about to commit" an offense as well as how a "victim" may be defined. It also only protected physical location information and not all location information such as which cell site—or series of cell sites—a caller is calling from. Moreover, in terms of permitted disclosures, the proposed law allowed the consent of the "user of the equipment" which could be defined as the cellular service provider and not the subscriber.[146] Indeed, who owns location information is not clear.[147] Carriers certainly own the gateways and the software that captures and records the location information and could therefore be authorized to release the information to LEAs without a court order and subscriber consent.[148] At any rate, while the bill certainly ad-

---

tal Privacy Act of 2000. H.R. 4987, 106th Cong. (2000) (introduced by Rep. Bob Barr (R-Ga)) (amending 18 U.S.C. §§ 2703, 2515, 3123).

145 H.R. 5018.

146 Whether the term "user" meant subscriber or carrier was, in fact, debated in the context of Caller ID in order to determine whose consent was required for a trap and trace. *See* 136 CONG. REC. E784 (daily ed. Mar. 22, 1990) (introduced by Rep. Kastenmeier).

147 *See* Matt Hamblen, *Ensuring Portable Privacy*, COMPUTERWORLD, Dec. 11, 2000, at 46.

148 Even if carriers are not defined as users here, they may be able to disclose the information without a court order or subscriber permission. Section 212 of the USA Patriot Act of 2001 (amending 18 U.S.C. § 2702) permits ISPs to voluntarily hand over content and non-content information to law enforcement with no need for any court order or subpoena if the provider has a reasonable belief "that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay." *Id.* (amending 18 U.S.C. § 2702(b)(6)(C)). Additionally, a recent Supreme Court ruling suggests that even hackers and others may be able to disclose information. In *Bartnicki v. Vopper*, 53 U.S. 514 (2001), the Court held that anti-wiretapping laws violate the First Amendment by prohibiting all disclosures of intercepted information, particularly when the banned information is of significant public concern. Essentially, information of

dressed the issue of location privacy and would have bolstered protection, it did not go beyond the House Judiciary Committee. Subsequent bills have focused on commercial and private use concerns, and not the issue of government access.[149]

B. *Technological Solutions*

In the meantime, technological solutions may rise to challenge the unrestrained surveillance. Currently, few mobile tools are location-aware, and most service providers are not yet archiving the data. With the impending deadline for full E911 compliance and implementation, however, carriers will soon have in place location information technology that will only get better in terms of precision and efficiency, particularly as they realize its marketability for commercial purposes. Yet as this technology improves, so will the opportunity for law enforcement to gain extensive and detailed location information. In response, privacy protection technologies will likely develop to afford users varying levels of privacy. For example, one company expects to sell prepaid disposable phones, which would certainly provide users privacy protection akin to calling anonymously from a phone booth. Qualcomm's "Snap Track" is supposed to incorporate a small switch on the phone to allow users to choose if they want their location transmitted.[150] Meanwhile, service providers are considering offering subscribers an opt-out location feature. Unfortunately, these privacy-enhancing technologies, or "PETs," may give users a false sense of security. Location information will still be maintained for billing and other purposes, and law enforcement will continue to gain access. Hence, citizens need to be educated in how their call location information may be gathered and used.

CONCLUSION

It was Supreme Court Justice Brandeis who once spoke of the "right to be let alone" as "the most comprehensive of rights and the

---

public interest may be lawfully distributed, even if it is obtained through the illegal interception of a telephone call.

149 Two bills introduced in 2001 require providers to restrict the collection and use of location information. *See* Wireless Privacy Protection Act of 2001, H.R. 260, 107th Cong. (2001) (introduced by Rep. Rodney Frehlinghuysen (R-NJ)) (amending 47 U.S.C. § 222) and Location Privacy Protection Act of 2001, S. 1164, 107th Cong. (2001) (introduced by Sen. John Edwards (D-NC)) (amending 47 U.S.C. § 222). Neither bill restricts government access, though. The Senate bill, in fact, permits the collection, use, and disclosure to "comply with an appropriate court order." Unfortunately, it allows for this to occur "without prior notice," meaning surveillance would occur without targets knowing their location was being monitored.

150 *See* Workshop, *supra* note 24.

most valued by civilized men."[151] Indeed, Americans have long enjoyed a constitutional right to travel, speak and associate freely, while the courts have increasingly recognized the right to privacy as being among those rights rooted in the Constitution. The Fourth Amendment specifically protects citizens from government searches and seizures. Certainly, unrestrained governmental monitoring or tracking of citizens via their cell phones or other wireless devices poses a serious threat to this nation's fundamental privacy rights.

As the number of people using cell phones rapidly grows each year, more Americans may become the subject of government tracking. While these citizens would be shocked to discover that their government can track their location without probable cause, most may never even know about the surreptitious monitoring. In the absence of a judicial decision recognizing an expectation of privacy in call location information, new legislation guaranteeing protection should be passed.

[151] Olmstead v. United States, 277 U.S. 438, 478 (1928).