Harvard Journal of Law & Technology
Volume 18, Number 1 Fall 2004

WHO KNOWS WHERE YOU'VE BEEN? PRIVACY CONCERNS REGARDING THE USE OF CELLULAR PHONES AS PERSONAL LOCATORS

TABLE OF CONTENTS

I. INTRODUCTION

A number of women are raped over the course of several hours one evening. The police have scant few details. It is possible that the perpetrator's first name is Tom, and that he may drive a late 1990's model Ford Taurus. After combing through the motor vehicle records for Toms with a Taurus, the investigators find someone who fits the bill and who also lives close to where the rapes occurred. While the suspect claims that he was at home after midnight on the night of the crimes, the police obtain his cell phone records in an effort to debunk the alibi. The records show several calls made after midnight. The calls themselves may not be incriminating, but the records reveal that they were not made from his apartment.

The preceding scenario played itself out on a recent episode of NBC's *Law & Order: Special Victims Unit*.[1] Did Hollywood contrive a plot device, or does art truly imitate life? Can cell phone carriers provide records that reveal the location of their subscribers? How precisely can cell service providers locate their customers? How much of that information is currently available to law enforcement officials

1. *Law & Order: Special Victims Unit* (NBC television broadcast, Nov. 30, 2004).

with and without a warrant? What information *should* be available to law enforcement?

II. CELL PHONES AND LOCATION INFORMATION — HOW IT WORKS

Cell service providers in the United States have been dealing with the problem of providing location information for years. In 2003, an estimated half of the 150,000 emergency calls placed per day to 911 were from cell phones.[2] While the wired telephone system immediately provides a 911 operator with location information, emergency calls from cell phones are not as easy to pin down. The difficulties presented by cell phone emergency calls led the Federal Communications Commission ("FCC") to set a deadline after which cell service providers must supply location information so that emergency callers can be located within 150 meters.[3] Providers typically can "pinpoint" the locations of their subscribers either by using global positioning system ("GPS") technology or signal triangulation.

Global positioning technology enables providers to pinpoint the position of a GPS-enabled cell phone anywhere on the globe. GPS works by measuring the time it takes for a signal to travel the distance between satellites and a cell phone's GPS chip. When the GPS chip receives four synchronized signals from GPS satellites, it can calculate a three-dimensional location that is accurate to within twenty meters. However, GPS does have certain disadvantages. Because the system depends on receiving information from satellites, it does not perform well when trees, buildings, or other barriers obstruct access.[4]

By contrast, locating cell phones by means of signal triangulation requires the use of information obtained by a cell service provider's cell towers. Each tower in a provider's network is equipped with radio intercepts that receive signals from any active cell phone. When two or more of these towers receive signals from the same phone, the towers are able to compare the signals and locate the unit in one of two ways: Time Difference of Arrival ("TDOA") or Angle of Arrival ("AOA").

When a cell phone connects with a provider's tower using a TDOA system, the tower measures the amount of time it takes for the signal to leave one location and reach the other. If the cell phone originates the contact (by making a phone call, for example), the

2. *Enhanced 911 Bill Passes House*, THE ALMANAC (Nov. 19, 2003), *at* http://www.almanacnews.com/morgue/2003/2003_11_19.calls.html.

3. 911 Service, 47 C.F.R. § 20.18 (2004) (requiring that licensees "achieve 95 percent penetration of location-capable handsets among [their] subscribers" by December 31, 2005).

4. *See* Smithsonian National Air and Space Museum, How Does GPS Work?, *at* http://www.nasm.si.edu/exhibitions/gps/work.html (last visited Dec. 3, 2004).

tower measures the time it takes the signal to get from the phone to the tower. Likewise, when the cell provider initiates the contact (by notifying a user of an incoming call), the tower measures the time it takes for the signal to get from the tower to the phone. These time measurements make it possible to estimate the distance between the tower and the phone. When more than one tower can do so, an algorithm allows the system to determine coordinates corresponding to the phone's latitude and longitude.[5]

Much like the TDOA system, angle-of-arrival technology uses signals between the cell tower and wireless phone to determine location. Rather than measuring the time it takes for the signal to travel between the two positions, however, the tower records the angle at which a phone's signal arrives at the station. When multiple towers receive signals, the system can compare the angles of arrival and thus triangulate the relative location of the cell phone.[6]

Even when users are not making or receiving calls, cell phones communicate with the nearest cell tower to register. Each unit has a Mobile Identification Number ("MIN") — the ten-digit number another caller dials to call a cell phone — and an Electronic Serial Number ("ESN") — a unique, unchangeable number assigned by the manufacturer. In order for a cell phone provider to carry outgoing calls and deliver incoming calls efficiently, phones must periodically notify the cell network of their locations. Once a unit registers its MIN and ESN with a particular cell, the system sends incoming calls directly to that cell. Given the inherently mobile nature of cell phones, units update their registration periodically so that the database is current. If a user has moved to another cell location, the unit re-registers there. If you have turned off your phone, the registration with a particular cell expires. It is unclear, however, whether cell service providers maintain records of these registrations.[7]

As people come to rely even more heavily on cell phones, service providers will continue to upgrade tower locations. In urban areas, the number of towers and their sectioning into directional "faces" (north face, south face, etc.) gives providers access to quite accurate location information. While making a single phone call, your signal can move between different cell towers or faces on a single tower, creating a virtual map of your movements. In rural settings, the location information available to providers is significantly less accurate simply because fewer towers are available. In some areas, cell service is provided by a single tower covering several hundred square miles. Nei-

5. *See* Bell South, How 911 Works, *at* http://contact.bellsouth.com/email/bbs/phase2/how911works.html (last visited Dec. 3, 2004).

6. *See id*.

7. *See* Marshall Brain & Jeff Tyson, How Cell Phones Work, *at* http://www22.verizon.com/about/community/learningcenter/articles/displayarticle1/0,1727,1008z2,00.html (last visited Dec. 3, 2004).

ther TDOA nor AOA techniques can triangulate locations in such circumstances.

III. LAW ENFORCEMENT & CELLULAR LOCATION INFORMATION

A variety of recent incidents suggest that cell location technology can be a powerful tool for law enforcement authorities.

On April 21, 2004, someone stole a car with a five-year-old girl inside while her mother visited with a relative. Though the woman had kept the keys in the ignition, she had fortunately also left her cell phone in the car. When she realized that the car and child were missing, she called the cell phone and the child answered. Using the cell tower triangulation information, the police were able to locate the car and child — both unharmed — within half an hour.[8]

After killing two Georgia real estate agents in November 2003, Stacey Ian Humphreys fled from authorities on foot, rented a car, and embarked on a road trip to Wisconsin. Throughout his journey, U.S. Marshals tracked his movements by monitoring his cell phone usage until a police officer recognized the rented vehicle and began a high-speed pursuit that ended with the suspect's capture.[9]

That same month, missing North Dakota college student Dru Sjodin's last cell phone call was processed from a cell tower in the vicinity of Crookston, Minnesota, twenty-five miles from her home in Grand Forks. The phone call led detectives to focus on a suspect who lived with his mother in the same area and had just been released from a twenty-three year sentence for rape, kidnapping, and assault. When DNA matching the victim was found in the suspect's car, their initial suspicions were confirmed. Alfonso Rodriguez, Jr. will be tried in federal court for the kidnapping and murder.[10]

In March of 2004, a Vancouver, Washington woman was shot and killed in her car. Though her ex-boyfriend was immediately a suspect, he told police that he was not in the area at the time of the murder. However, cell phone records proved otherwise. The cell tower information for his calls placed him within blocks of the scene of the crime both before and three minutes after the shooting. Records further indicated that during the actual murder, he likely had the phone turned off. Prosecutors argued this was also inculpatory in that

8. *See Girl, 5, Found Safe as Man Steals Car*, ROCKY MTN. NEWS, Apr. 22, 2004, at A18.

9. *See* Don Plummer, *Cellphone Betrays Cobb Fugitive*, ATLANTA J.-CONST., Nov. 9, 2003, at A1.

10. *See* Chuck Haga, *Sjodin's Body Found; Officers Find Remains in Ravine Near Crookston*, MINNEAPOLIS STAR TRIB., Apr. 18, 2004, at A1.

someone who was secretly stalking a victim would not want a cell phone call to alert the victim to his presence.[11]

In perhaps the most widely publicized trial of the year, the prosecution of Scott Peterson for his wife Laci's murder, the state introduced cell phone records in order to establish the defendant's whereabouts. Though Peterson maintained that he left the house on the morning of the murder at 9:30, cell phone records placed him at home until 10:08. In cross-examination, defense attorneys pointed out that cell phone records are not intended to pinpoint the caller's location, but an investigator testified that he did three "test runs" replicating the movements prosecutors believed Peterson had made on the morning of Laci's murder. As the prosecution expected, the investigator's calls were first picked up on a cell tower near the Peterson home and then transferred to a nearby tower as he moved toward Peterson's warehouse.[12]

In each of these investigations, law enforcement authorities used cell phone records that cell phone owners themselves had effectively created as a result of making outgoing calls or accepting incoming ones. Given the Supreme Court's decision in *Smith v. Maryland* that a defendant has no expectation of privacy as to the numbers he dials when using a phone,[13] it is no surprise that law enforcement authorities can obtain at least certain information about cell phone calls without a warrant. However, what are the constraints on such access?

IV. COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT OF 1994

Prior to the advent of cell technology, telephone communications did not pose a significant problem for law enforcement authorities because the origin and destination of calls was dictated by physical phone lines. A search order for a wiretap intercept authorized investigators to listen to and record conversations on telephone lines believed to be used by a particular suspect or suspects.[14] Pen register orders gave the government access to the numbers dialed on a particular phone line, while trap and trace orders captured incoming call

11. *See* Holley Gilbert, *Vancouver Man Is Arrested In Shooting Death of Ex-Girlfriend*, PORTLAND OREGONIAN, Apr. 30, 2004, at B1.

12. *See* Diana Walsh & Stacy Finz, *The Peterson Trial; Defendant Lied Often, Recorded Calls Show; Supporters Misled About Whereabout*s, SAN FRANCISCO CHRON., Aug. 26, 2004, at B1. When a cell customer approaches the outer reaches of a tower's signal area, it polls the surrounding towers, asking them to search for the caller's signal. When another tower registers that the caller is within its range, the original tower transfers the call to the new tower. Obviously, the more cell towers available within an urban area, the more precisely one's movements can be tracked via cell transfers. *See supra* note 7.

13. 442 U.S. 735, 742 (1979).

14. 18 U.S.C. § 3121 (2000 & Supp. I 2001).

origination information whenever an outsider called a specified line.[15] As Justice Brandeis noted in his 1928 dissent in *Olmstead v. United States*, however, "[s]ubtler and more far-reaching means of invading privacy have become available to the Government . . . . The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping."[16]

The increasing popularity of cell phones has indeed forced authorities to reevaluate search and seizure rules. Six percent of Americans rely on a cell phone alone for their telecommunications, and more than 170 million own cell phones.[17] Given the inherent portability of the devices, most owners keep their phones on or near their persons. Cell phones are accordingly much more "tied" to a particular individual than wired lines. For example, if you live with roommates and have a landline in your house or apartment, any or all of your roommates could make and receive phone calls on the phone line at any given time. Conversely, cell phones are more akin to a private line installed only in your room; it is much more likely that you will be the sole user of the phone. Perhaps more worrisome is the location information available to the cell phone carrier.[18] The reality that people carry their cell phones on their persons means that cell phone tracking technology potentially offers a detailed view of a given subscriber's movements rather than simply providing call-identifying information.

In 1986, legislators attempted to strike "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies"[19] by enacting the Electronic Communications Privacy Act ("ECPA"), but the statute actually extended law enforcement's authority to intercept cell communications.[20] In October of 1994, Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA") to enumerate the obligations of telecommunications carriers to aid in intercepting digital communications.[21] Among other things, CALEA requires carriers to enable law enforcement agents "to access call-identifying information that is reasonably available to the carrier . . . before, during or immediately after the transmission of a wire or electronic communication."[22] However, the statute specifies that "with regard to information acquired solely

15. 18 U.S.C. § 3123 (2000 & Supp. I 2001).

16. 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting).

17. Jane Roh, *Are Cell Phones Skewing Polls?*, FOX NEWS (Oct. 24, 2004), *at* http://www.foxnews. com/story/0,2933,136394,00.html.

18. *See supra* notes 2–7.

19. S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

20. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.) (extending the baseline regulatory scheme for "wire" communications to "electronic" communications as well).

21. Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010).

22. 47 U.S.C. § 1002 (a)(2) (2000).

pursuant to the authority for pen registers and trap and trace devices . . . such call-identifying information shall not include any information that may disclose the physical location of the subscriber."[23]

This restriction concerning the physical locations of callers suggests a reluctance to provide law enforcement with detailed tracking information. When considering the statute in *United States Telecom Ass'n v. FCC*,[24] the D.C. Circuit appeared to adopt a similar attitude. The court cited the FCC's rejection of a New York Police Department proposal that would have "required triangulating signals from multiple cell antenna towers to pinpoint a wireless phone's precise location throughout a call's duration."[25] The FCC found that providing law enforcement with triangulation capabilities "pose[d] difficulties that could undermine individual privacy."[26] The agency in turn suggested that "a more generalized capability that will identify only the location of a cell site, and only at the beginning and termination of the call, will give L[aw] E[nforcement] A[uthoritie]s adequate information," and it further noted that the FBI, the DOJ, and the telecommunications industry had already agreed that such an arrangement would be sufficient.[27]

One must assess these regulations in light of the Fourth Amendment, which protects "[t]he right of the people to be secure in their persons, houses, papers and effects. . . ."[28] The Supreme Court made clear in *Katz v. United States* that the Fourth Amendment protects people rather than places.[29] As Justice Harlan observed in a concurring opinion, courts determining whether one's rights have been violated must apply a two-pronged test. First, the claimant needs to demonstrate that he or she had a subjective expectation of privacy in the place searched. If so, the question remains whether society recognizes that expectation as reasonable.[30]

Where does this leave cell phone users? While almost everyone is presumably aware in a general sense that making cell calls entails sending and receiving information via cell towers, few customers are likely to appreciate the specificity of the location information available to service providers and the fact that the companies can retain it indefinitely. Even sophisticated cell phone owners may think that they can avoid providing location information by turning off their GPS chips, not realizing (or forgetting) that triangulation can provide gen-

---

23. *Id*.
24. 227 F.3d 450 (D.C. Cir. 2000).
25. *Id*. at 464.
26. *Id*. (quoting *In re* Communications Assistance for Law Enforcement Act, 14 F.C.C.R. 16794, ¶ 46 (1999)).
27. 14 F.C.C.R. at ¶ 46.
28. U.S. CONST. amend. IV.
29. 389 U.S. 347, 351 (1967).
30. *Id*. at 361 (Harlan, J., concurring).

eral location information. How then can a cell phone customer demonstrate his subjective expectation of privacy in location data, and is society prepared to accept that expectation of privacy as reasonable? According to the *Katz* majority, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[31] Since the FCC's mandate focuses only on the origination and termination of calls,[32] does a citizen have a subjective expectation of privacy if he does not dial or answer his cell phone? Is choosing not to make or receive a phone call a manifestation of your intent to keep your cell tower location information private?

V. *UNITED STATES V. FOREST*[33] — CELL PHONES AS TRACKING DEVICES

In March 2001, defendants Forest and Garner were identified by the DEA as active cocaine traffickers. The DEA obtained court orders to intercept communications over both defendants' cell phones and required Sprint "to disclose to the government all subscriber information, toll records, and other information relevant to the government's investigation."[34] Though drug agents attempted to conduct visual surveillance of the defendants, they were not able to keep them in sight. Rather than waiting for one of the defendants to place a call and tracking it using cell tower information, the DEA simply dialed Garner's cell phone several times over the course of the day without allowing it to ring. The agents "used Sprint's computer data to determine which transmission towers were being 'hit' by Garner's phone."[35] This general location information enabled the DEA to reestablish visual contact with the defendants' vehicle.

In seeking to suppress the data that the DEA had obtained, Garner contended that the agents had "effectively turned his cell phone into a tracking device" by dialing his number and obtaining cell tower information.[36] The Sixth Circuit rejected all of the appellant's arguments. First, the court concluded that even if the signals transmitted between the cell towers and Garner's phone amounted to "communications," they were certainly "electronic" rather than "wire" or "oral."[37] Therefore, no suppression remedy was available.[38] Second,

31. *Id*. at 351.
32. *See supra* notes 26–27.
33. 355 F.3d 942 (6th Cir. 2004), *cert. denied*, 125 S. Ct. 174 (2004).
34. *Id*. at 947.
35. *Id*.
36. *Id*. at 948.
37. *Id*. at 949.
38. *Id*. (citing 18 U.S.C. § 2518(10)(a) (2000)).

the court adopted the D.C. Circuit's conclusion that the ECPA provision concerning tracking units[39] does not bar evidence obtained through the use of such devices.[40] Finally, the court relied heavily upon *United States v. Knotts*[41] in holding that the defendants had no Fourth Amendment claim.[42]

In *Knotts*, law enforcement agents placed a beeper in a container transported by the defendants and used it as a tracking device.[43] After the defendants began driving evasively and the officers accordingly lost visual contact, the authorities used the tracking device to determine the defendants' ultimate destination.[44] The Supreme Court held that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[45]

Since the DEA agents had likewise tracked the movements of Forest and Garner on public highways, the Sixth Circuit ruled that Garner had "no legitimate expectation of privacy in the cell-site data because the DEA agents could have obtained the same information by following Garner's car."[46]

VI. A *KATZ* ANALYSIS: REASONABLE EXPECTATIONS OF PRIVACY WITH RESPECT TO CELL PHONE INFORMATION

Even though the defendants traveled on public highways, *Forest* raises serious questions about the limits of the authority of law enforcement agencies to access and use cell tower data. Using the *Katz* two-pronged test, one can certainly argue that Forest and Garner had both a subjective and an objective expectation of privacy.

First, the information that the DEA obtained was arguably outside the definition in the FCC/CALEA regulations, for the data was not "call-identifying" in the strict sense of the word. Indeed, Garner neither placed nor answered any calls that provided the agents with cell tower location information. The decision not to make or answer phone calls moreover supports an argument under *Katz* that the defendants should have constitutional protection because they sought "to preserve [their cell phone information] as private, even in an area accessible to the public."[47] Regardless whether they understood the implications

39. 18 U.S.C. § 3117 (2000).
40. *Forest*, 355 F.3d at 950 (citing United States v. Gbemisola, 225 F.3d 753, 758 (D.C. Cir. 2000)).
41. 460 U.S. 276 (1983).
42. *Forest*, 355 F.3d at 950–52.
43. 460 U.S. at 277.
44. *Id*. at 278–79.
45. *Id*. at 281.
46. *Forest*, 355 F.3d at 951.
47. *See supra* note 31.

under CALEA of making or receiving a phone call, the fact remains that Forest and Garner *refrained* from taking such actions. They therefore exhibited an expectation of privacy in their cell tower data.

While the Sixth Circuit held in *United States v. Meriwether* that there is no reasonable expectation of privacy when transmitting a message to a pager because a sender runs the risk that the message could be intercepted by anyone who has possession of the device,[48] the case is readily distinguishable. The *Meriwether* court itself commented that "[u]nlike [a] phone conversation where a caller can hear a voice and decide whether to converse, one who sends a message to a pager has no external indicia that the message actually is received by the intended recipient."[49] Extending the reasoning to *Forest*, Forest and Garner did not merely choose whether to transmit a receivable message or to converse upon hearing a voice. They instead elected not to initiate or receive *any* communication via their cell phones.

One can also argue under the second, objective prong of *Katz* that Forest and Garner had reasonable expectations of privacy. Though society no doubt recognizes the need for law enforcement agencies to conduct efficient surveillance and investigations, this does not necessarily mean that people expect their locations and movements to be monitored via cell technology. As discussed above, service carriers can determine this information with surprising ease whenever cell phones are turned on — even if users switch GPS functions to emergency-only mode.[50] Given current database and storage capacities, the door is open for an Orwellian scenario whereby law enforcement agents could monitor not just criminals, but anyone with a cell phone. If it sounds improbable, consider that commercial tracking services already provide real-time location information for families and businesses. On-line services like uLocate allow users to "[v]iew the locations of all family members on the web site or your phone," "[r]eview all the locations visited during a specified time frame," "[p]ermit [others] to view your location on a temporary basis," and "[b]e alerted when individuals arrive or depart from specified locations."[51] While society may be willing to accept the idea of collecting information associated with the origination and termination of calls, people are likely to reject the prospect of turning every cell phone into a tracking device.

48. 917 F.2d 955, 959 (6th Cir. 1990).
49. *Id*.
50. *See supra* text accompanying notes 2–7.
51. uLocate, *at* http://www.ulocate.com (last visited Dec. 3, 2004).

VII. A CALL TO LEGISLATORS

While the legislative process has always been slow to react to changing technology, the consequences that could arise from governmental abuse of cell phone data make it imperative for legislators to acknowledge and address the problem. Even if the FCC continues to interpret CALEA as limiting the scope of available information, Fourth Amendment protections are ephemeral at best. Without legislation that establishes specific requirements for cell data warrants, courts could easily extend *Forest* and allow intrusions into traditionally private areas like homes. Short of abandoning the technology altogether, the only means a cell phone owner has to avoid tracking is to switch off his phone.

The irony of the *Forest* opinion is that it relies heavily on *Knotts* for disposition, yet the Supreme Court's decision itself contains ominously prescient dicta relevant to this discussion. While acknowledging the respondent's concern that "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision," the Court reasoned that "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[52] It seems that this time has come.

52. United States v. Knotts, 460 U.S. 276, 283–84 (1983) (citing Zurcher v. Stanford Daily, 436 U.S. 547, 566 (1978)).