

# The Privacy Implications of Cellular Locationing

Mel Tsai

mtsai@eecs.berkeley.edu

CS294-5 Special Topics: Privacy

12/4/2002

## Abstract

*In order to implement Wireless-911, the Telecommunications Act of 1996 has mandated that all wireless carriers implement high-accuracy locationing for every cell phone user in the United States. This mandate is a major privacy concern for anyone who uses a cellular phone. Can the U.S. Government legally track your location? Can your wireless carrier track your location and sell your location data to others? This paper introduces the major privacy issues of cellular locationing and provides an overview of the applications of cellular locationing, the laws governing the use and dissemination of your cellular location, and some techniques to secure your privacy in an age where your location is no longer secret.*

## 1. Introduction

Most people would be surprised to find out that the government can legally track the location of your cellular call if they suspect you are involved in criminal activities. Indeed, the ubiquitous cellular phone owned by nearly 140 million subscribers [1] in the United States has become a powerful tool for the FBI and law enforcement. On the other hand, most cellular carriers today can only track your location within 2-3 miles, essentially to the nearest cellular tower. Pinpointing your location within only 2-3 miles is worrisome, but hardly a reason to throw away your cell phone. However, a 1996 law is about to change this.

A major goal of the Telecommunications Act of 1996, which updated the previous Communications Act of 1934, was to bring the standards of 911 calls made from cellular phones up to the level afforded by calls made from regular land-based phones. About 20 years ago, the “Enhanced-911” system was installed that allowed the name and location of any 911 caller to be automatically identified [2]. The previous 911 system relied upon callers identifying themselves to a

PSAP (public safety access point) operator. In order to route a cellular 911 call to the correct PSAP and automatically locate a cellular 911 caller, the current Enhanced-911 system needs a major overhaul. Thus, the “Wireless-911” initiative was borne out of the Telecommunications Act of 1996.

The valuable increase in public safety associated with Wireless-911 is clear. The CTIA estimates [3] that almost 57 million calls to 911 in 2001 were made from cellular phones (that’s nearly *two calls per second*). Indeed, a major selling point of cellular phones is the increased safety associated with carrying one at all times. So, in the interests of public safety, the Wireless-911 order requires all carriers to implement real-time, high-accuracy location tracking to their infrastructure.

As it turns out, the implementation schedule [4] for Wireless-911 was quite ambitious, and the FCC has since revised the schedule. Under the FCC’s original order, “Phase-I” of Wireless-911 required all carriers and local PSAP systems to correctly identify cellular 911 callers to the nearest cellular tower. While many carriers and PSAPs have complied with the Phase-I requirements (the deadline has long since passed), the considerable expense incurred by Phase-I implementation may force some carriers and PSAPs to give up on Phase I and move directly to Phase-II [5].

In Phase-II, carriers are required to increase the accuracy of locationing to roughly 50-350 meters, depending on the chosen location-tracking technology (carriers have a choice of several technologies, e.g. GPS- or network-based, each with different trade-offs). To date, the major wireless carriers such as AT&T, Verizon, Sprint, and Cingular have been slowly conforming to the Phase-II schedule, but they have all requested waivers and extensions for various deadlines of Phase-II. Nonetheless, based on the latest Phase-II reports, one can expect that the wireless carriers will

have 50+ meter accuracy for nearly all cellular 911 callers within 2-3 years.

Interestingly, if it were not for Wireless-911, the United States would be years away from implementing location-finding technology into our cellular infrastructure. Japan, on the other hand, is strongly adopting location-based technologies in a variety of contexts, mostly because streets in Japan do not have names [6]. Thus, while the U.S. is about to start grappling with the privacy and security implications of cellular locationing due to Wireless-911, Japan has already embraced the technology.

The potential impact on personal privacy due to the rollout of Wireless-911 is staggering. The government, which can already track your location with a court order to the nearest cellular tower, is about to be handed a high-accuracy tracking tool for law enforcement once Phase-II is complete. Given the U.S. Government's less-than-stellar track record of extending its reach in the interests of national security (e.g. Carnivore and the rumored Echelon system), it would not be surprising if they introduce legislation to begin monitoring the location of everyone in the United States and flag users with suspicious movement.

The potential commercial abuse of location-finding technologies is also concerning. What protection (legal or otherwise) do we have against carriers "selling" our location in real time? What prevents a location-based advertiser from spamming our cell phone with a coupon for a restaurant across the street? In general, what control do we have over the use and dissemination of our location for commercial interests?

The rest of this paper is organized as follows. In Section 2, a brief overview of the various location-finding technologies is given. Section 3 presents three main drivers in the U.S. for cellular location-based services: Wireless-911, commercial applications, and FBI and law enforcement use. Section 4 provides a brief history of the laws that govern the commercial and government use of cellular location data. Section 5 discusses several of the privacy concerns associated with this new technology and some ways for an individual to secure his/her own privacy. Finally, Section 6 concludes with some remarks about the true costs (both economic and societal) of location-based services.

## 2. Location-Finding Technologies

### 2.1. Manual Location Input

Currently, most users of wireless web browsers must enter their zip code to obtain local weather, sports, or traffic reports via WAP. This "manual location input" technique is effective, but cumbersome and often impractical in some situations. For example, it is often the case that users do not know their current zip code or even the city. Ideally, WAP-based information sites should be able to automatically determine the location of users.

### 2.2. Nearest Cellular Tower

Several wireless carriers have already integrated locationing to the nearest cellular tower. As long as users can be located to within a 5-10 mile area, many useful services (such as local weather and traffic) can be deployed. However, many future services will require more accuracy, which can be good (2-3 miles) in urban areas but poor in rural areas.

### 2.3. Network-Based Locationing

In the FCC's original implementation order for Wireless-911, network-based solutions to high-accuracy locationing were required for carriers. In this approach, the cellular towers are upgraded to support triangulation or trilateration of caller location based on signal strength, time-of-arrival (ToA), or angle-of-arrival (AoA) data [7]. Little or no modification to cellular handsets are required in this approach. Although many carriers have abandoned network-based solutions for Wireless-911, this is the current approach taken by Verizon, the largest wireless carrier in the United States.

### 2.4. GPS-Based Locationing

In May of 2000, the U.S. government eliminated "Selective Availability" (SA) in the global positioning system. SA was the intentional error introduced into GPS so that very high accuracy was achieved only for military use, and at unannounced times. With the removal of SA, this meant that GPS units could achieve accuracy to within 10-15 meters instead of the previous 100 meter accuracy. Today, with the widespread commercialization of GPS, the FCC has allowed wireless carriers to augment cellular handsets

with GPS receivers in order to implement Wireless-911, and several carriers are doing so. Carriers that choose GPS-based solutions must achieve somewhat higher accuracy for Phase-II Wireless-911 than carriers that choose network-based approaches.

Unfortunately, GPS solutions have their shortcomings. First, the GPS timing signal is easily blocked by dense foliage and walls, which can often render it useless indoors. Second, GPS receivers can add considerable cost, bulk, and power consumption to cellular handsets. Finally, GPS receivers can sometimes require several minutes to acquire a signal and report an initial location estimate.

### 2.5. Hybrid Techniques

Instead of purely network-based or GPS-solutions, some carriers are implementing hybrid network/GPS approaches to high-accuracy locationing. In general, hybrid approaches can offer superior performance to GPS-only solutions.

SnapTrack (<http://www.snaptrack.com/>) is an example of a hybrid system that uses the cellular network infrastructure to assist on-board GPS to acquire the signal faster, consume less power, and perform better indoors [8]. SnapTrack was recently acquired by Qualcomm and has been deployed under the name “gpsOne” to “millions” of CMDA handsets throughout Asia and the United States [9].

## 3. Applications of Cellular Locationing

### 3.1. Wireless-911

As discussed previously, the Wireless-911 mandate from the Telecommunications Act of 1996 has been the primary driver for cellular locationing in the United States. Interestingly, to highlight the importance of Wireless-911 deployment, the National Emergency Number Association (NENA) maintains a list of “Wireless-911 Tragedies” [10]. The list contains several poignant examples where high-accuracy locationing could have averted a tragic event. In one gruesome example, a woman who called 911 from her cellular phone was being stabbed to death by her ex-husband. According to the story, the police were unable to pinpoint her location until after she was dead.

### 3.2. Commercial Applications

There are obvious commercial applications for cellular locationing. In the past three years, many service companies have been started that are focusing on services such as:

- Location-sensitive advertising, e.g. “pull advertising” with “wireless coupons”
- Street navigation
- Local traffic and weather reports
- Mobile yellow pages and enhanced 411 services
- Enhanced roadside assistance
- Remote patient monitoring
- Location-sensitive billing, e.g. discounted calling plans if you call within 100 meters of your home
- Facility & campus tours
- Conference-floor navigation
- Finder applications: restaurants, movies, ATMs, gas stations, hotels, local attractions

Relatedly, as of this writing, there are 14 companies that comprise the Wireless Location Industry Association (WLIA) [11]. The WLIA has a variety of roles in the locationing arena, including business model and privacy policy development for its members.

### 3.3. FBI and Law Enforcement Surveillance

Law enforcement agencies (LEAs) have several legal surveillance tools at their disposal. An obvious tool is the wiretap, where a LEA can listen to a conversation placed by a suspected criminal after obtaining a court order. Pen registers, another surveillance tool, capture the outgoing phone number that was dialed from a particular phone, but do not reveal call content information. Similarly, traps and traces reveal the phone number of an incoming call.

By law, LEAs can also obtain the location of a caller. In the past, the location of a caller could be determined based on the originating phone number. The 1994 Communication Assistance for Law Enforcement Act (CALEA) was passed so that emerging communication systems (such as cellular wireless) would continue to facilitate surveillance tools such as wiretaps, pen registers, and caller location. Although the interpretation of CALEA has come under fire several times (see Section 4.2 below), the most recent rulings affirm that, under the provisions of CALEA,

wireless carriers must supply the location (with the highest available accuracy) of a cellular caller to LEAs when requested with a court order.

## 4. Location Data and the Law

In order to properly evaluate the privacy implications of cellular locationing, it is important to understand the history of laws governing the use of location data.

### 4.1. Commercial Laws

The Telecommunications Act of 1996, the same legislation that mandated Wireless-911, includes a new section (47 U.S.C. § 222) that explicitly limits the use and dissemination of customer proprietary network information (CPNI). The CPNI includes personally-identifiable information such as the customer name, address, phone numbers dialed, and calling plan details. (In 1999, the legal definition of the CPNI in § 222 was modified to explicitly include caller location [12]). Under § 222(c)(1), a carrier requires “approval of the customer” if it wants to use the CPNI for purposes other than the communications service, e.g. selling the CPNI to a third party.

When the FCC released its original implementation order for Section 222, controversy erupted over the definition of “customer approval.” According to the FCC’s 1998 CPNI Order [13], § 222 required an “opt-in” policy for carriers. The FCC argued that an opt-out policy constitutes implied consent, which is not “customer approval.” However, the FCC’s requirement for an opt-in approach was challenged [14] by Qwest Communications (then U.S. West). Qwest contended that the opt-in policy violated protected *commercial speech* under the First and Fifth Amendments. As a result, the Tenth Circuit court vacated the opt-in policy of the CPNI Order in August 1999. Several hearings and rulings have followed since, but the most recent [15] FCC regulations regarding the CPNI have been altered to include an opt-in policy for “third parties,” but an *opt-out* policy for “affiliates.”

Based purely on the above discussion, one would assume that carriers can freely distribute our wireless location to affiliates with nothing more than an opt-out policy. However, the laws regarding location data are presently unclear. In 1999, the Wireless Communications and Public Safety Act (the “911 Act”) was passed

that further amended § 222. This amendment, § 222(f), distinguishes between the CPNI and a caller’s location, requiring “express prior authorization of the customer” if wireless carriers are to distribute caller location. Seeking to further clarify the unresolved implementation details and requirements set forth by § 222(f), the CTIA (backed by several privacy groups including the CDT) petitioned the FCC to issue a set of rules for carriers to implement § 222(f). Unfortunately, in July 2002 the FCC ruled [16] that § 222(f) requires no further clarification, and believes it is better to “vigorously enforce the law as written.”

Due to the FCC’s failure to explicitly clarify § 222(f), it is unclear to what extent the wireless carriers and location-based service providers must legally protect subscriber privacy. Surely, wireless carriers must adopt an “opt-in” policy for location-based services, but once a subscriber opts-in, what protections under § 222(f) remain? For example, in the future, will these “opt-in” policies become free-for-all agreements that give wireless carriers free and unabated use of location data, similar to the notorious end-user license agreements in today’s software? Does § 222 really protect subscriber location privacy at all? For now, the laws regarding protections after a subscriber “opts in” are non-existent.

Fortunately, while only weak subscriber protection exists today, there are several privacy groups [17], industry associations [18], and legislators that are working to further secure our location data from potential corporate abuse. For example, in July 2001, Senator John Edwards (D-NC) introduced the Location Privacy Protection Act (S.1164), which has since been referred to the Senate committee on Commerce, Science, and Transportation. If passed, this bill will significantly extend provisions of § 222(f) to include explicit restrictions on corporate use and distribution of location data. It also provides safeguards for unauthorized access to location data and a means for individuals to correct errors in location data.

As a final note on commercial laws for cellular locationing, the FCC’s most recent rulings [16] regarding § 222(f) have left open the possibility of further *state regulation* of CPNI and location data sharing. As a result, in November 2002, the state of Washington adopted [19] the nation’s strongest opt-in rules for the CPNI. Under these rules, the CPNI and location data can only be shared among companies under a common

ownership. Unfortunately, it is unknown whether other states will follow suit.

#### 4.2. Government Laws

As discussed in Section 3.3, the 1994 Communication Assistance for Law Enforcement Act (CALEA) gives a law enforcement agency the power to perform wiretaps, pen registers, traps, traces, and determine *call-identifying information* (which includes location) of wireless callers via a via a court order. In response to CALEA, the Telecommunications Industry Association (TIA) published what became known as the “J-Standard” [20] in 1997, which set guidelines for how carriers must implement CALEA’s surveillance provisions.

Several controversies arose from the J-Standard (from both the FBI and the carriers), but one of them was the requirement that wireless carriers supply the location of a cellular call to law enforcement. The heart of this dispute was over the legal definition of “call-identifying information.” Section 102 of CALEA defines call-identifying information to be “dialing or signaling information that identifies the *origin*, direction, destination, or termination of each communication.” As it turns out, the Center for Democracy and Technology (CDT) argued that the true meaning of call-identifying information in CALEA was *only the telephone number*, not the location. Although they had some compelling arguments to support this claim, the courts have concluded that LEAs have the right to obtain a caller’s location under CALEA.

### 5. Privacy Concerns of Locationing

High-accuracy locationing is quickly becoming a reality for all wireless subscribers in the U.S. It is clear that the limited “opt-in” laws of 47 U.S.C. § 222 will provide little or no protection against an unscrupulous company. Wireless subscribers may quickly find themselves in a quandary when subscribing to a location-based service. If they opt-in to the service, they could open themselves to potential abuse, but if they do not opt-in, they will miss out on the valuable array of location-based services that may become tomorrow’s killer application of mobile phones.

What types of abuse may subscribers experience? On the one hand, the abuse could be innocuous pestering from “mobile spam” as you walk by a restaurant or

department store. On the other hand, the abuse could be as sinister as corporate espionage, whereby a company monitors and tracks the location of key members of their competition. Surely, the possible scenarios of commercial privacy abuse of locationing could fill an entire report.

The potential for government abuse is perhaps even more concerning. What if the INS required all U.S. permanent residents from middle-eastern countries to be constantly tracked via their cell phone? What if the location history of everyone in the U.S. was stored in a large database, ready to be used in the interests of national security? This situation is closer to reality than one might think. Under current law, a law enforcement agency has a legal right to subpoena the records kept by a mobile location-based service. In addition, it is already well known that the FBI is asking the FCC [21] to require carriers to retain CPNI information (even after a subscriber discontinues their service) for law enforcement use.

Abuse does not have to come solely from the government or carriers. Cell phone cracking and mass-spamming has been a minor annoyance in the U.S. and Japan, but the potential for cracking will only increase as the technology proliferates. A subscriber’s location is a particularly sensitive (and valuable) piece of information, and could become a prized target for hackers. This problem is exacerbated by the imminent arrival of mobile viruses [22].

### 6. Conclusion: Securing Your Privacy

Cellular phones have become completely integrated into the lives of millions worldwide. The harsh reality is that *complete* location privacy can only be achieved by throwing away your cellular phone, and even then, there are other (manual) ways for someone to track you.

For the time being, opt-in policies protect your cellular location from wireless services other than 911 and criminal investigations. But, until the laws change, choosing not to opt-in to location-based services is currently the best and only way to stop commercial abuse of your location data.

Fortunately, help may come from both the equipment vendors and the wireless carriers. Verizon, for example, sells a GPS-equipped cellular phone from Samsung that allows users to manually disable the on-board GPS tracking. The GPS feature is automatically

re-enabled when making a call to 911, but for normal calls your location will no longer be accurate to 50 meters.

In some respects, the wireless carriers have an economic interest in securing the privacy of customers. Customer churn is a constant headache among carriers, and the carriers will do anything to keep customers subscribed to their lucrative monthly plans. An average subscriber may not be too concerned about privacy in other contexts, but when told that their location can be tracked with high accuracy, customers might think twice about this clear threat to personal privacy and might go shopping elsewhere. For a case in point, recall the consumer backlash due to Intel's controversial Pentium-III serial numbers. Ironically, this feature was introduced in the interests of increasing online security. Once consumers caught on to the privacy implications of unique CPU serial numbers, several utilities and motherboard drivers were released that could disable this "feature." Ultimately, after the bad press, Intel quietly dropped [23] the serial numbers from the Pentium-4.

At the very least, in order to successfully deploy location-based services, carriers must downplay the potential privacy impact, or (better still) adopt strong privacy protection policies for their customers. An possible approach is the introduction of strong and easy-to-understand "privacy profiles" that give the user complete control over the use of their location. The WLIA's strong privacy policy [18] is an example where the locationing industry realizes that privacy protection is a key factor in its success.

Unfortunately, the dark side of Wireless-911 is the considerable expense incurred by carriers in order to deploy high-accuracy locationing. Wireless carriers, which are constantly searching for ways to differentiate their products and services, may quickly want to force location-based services down the throats of customers in order to recoup their costs for Wireless-911. So, in the near future, carriers will carefully weight the advantages of securing privacy against the strong economic need to deploy wireless locationing services. Only time will tell which factor will win, but it is unlikely that strong privacy will be the norm for mobile phone users in the future.

## 7. References

- [1] Cellular Telecommunications and Internet Association (CTIA), Semi-annual Wireless Industry Survey Results, June 1985 - June 2002. <http://www.wow-com.com>
- [2] Bellsouth Corporation, "How 911 Works," <http://contact.bellsouth.com/email/bbs/phase2/how911works.html>
- [3] CTIA Press Release, "Wireless Emergency Service Calls Near 156,000 Per Day, 108 Calls per Minute," May 22, 2002.
- [4] Federal Communications Commission, "FCC Wireless 911 Fact Sheet," <http://www.fcc.gov/911/enhanced/>, January 2001.
- [5] Dispatch Monthly, "Wireless 911," Online Infosite, <http://www.911dispatch.com/>
- [6] Carlos Camacho, "Location-Based Services in Japan," *all-NetDevices.com*, January 2001.
- [7] A. Savvides, C. Han, M. Strivastava. "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors," SIGMOBILE 2001.
- [8] Walter Bell, "SnapTrack, Inc. FCC Location Roundtable," Overview Powerpoint Presentation, June 28, 1999.
- [9] Qualcomm, Inc., "QUALCOMM Announces Over One Million Subscribers Served by gpsOne-Enabled Devices," Corporate Press Release, May 8, 2002.
- [10] National Emergency Number Association (NENA), "Wireless-911 Tragedies," <http://www.nena9-1-1.org/Wireless911/Tragedies.htm>
- [11] Wireless Location Industry Association (WLIA), <http://www.wliaonline.com/>
- [12] Wireless Communications and Public Safety Act of 1999 (the "911 Act"), Pub. L. No. 106-81, enacted Oct. 26, 1999, 113 Stat. 1286
- [13] CPNI Order, 13 FCC Red 8061.
- [14] U.S. WEST v. FCC, 182 F.3d 1124.
- [15] FCC-02-214, Released July 25, 2002
- [16] FCC-02-208, Released July 24, 2002
- [17] J. Cuellar, J. Morris, D. Mulligan, "Geopriv requirements," IETF draft, November 2002.
- [18] Wireless Location Industry Association, "Adopted WLIA Privacy Policy," First Revision, <http://www.wliaonline.com/>, 2002.
- [19] Washington State, Docket No. UT-990146, General Order No. R-505, November 7, 2002.
- [20] J-STD-025, "Lawfully Authorized Electronic Surveillance," Committee T1 and the Telecommunications Industries Association, December 1997
- [21] Reply Comments of the Electronic Privacy Information Center (EPIC), CC Docket No. 96-115

[22] Reuters, "Experts warn of mobile viruses," August 27, 2002

[23] D. McCullagh, "Intel Nixes Chip-Tracking ID," *Wired News*, April 27, 2000