

House Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil
Liberties
Hearing on ECPA Reform and the Revolution in Location Based
Technologies and Services

Testimony of Professor Matt Blaze

June 24, 2010

1. Introduction and Background

Thank you for the opportunity to provide some background about location technology in current and emerging wireless networking. It is a great honor to be here, and I hope my remarks will be helpful in understanding how location information is calculated and the direction that this important and yet rather complex technology is taking. I offer my testimony today on my own behalf and do not represent any other party or organization.

I am currently an associate professor of computer and information science at the University of Pennsylvania in Philadelphia, where I serve as director of the Distributed Computing Laboratory and conduct research on computer security, cryptography, network communication, and surveillance technology. Prior to joining the faculty at Penn, I was for 12 years a member of the research staff

at AT&T Labs (previously known as AT&T Bell Labs) in New Jersey. I have a PhD in computer science from Princeton University, a Masters degree from Columbia, and I completed my undergraduate studies at the City University of New York.

A focus of my research is on the properties and capabilities of surveillance technology (both lawful and illicit) in the context of modern digital systems and communications networks. This research aims to strengthen our critical infrastructure against criminals and other unauthorized eavesdroppers and to help ensure that authorized surveillance systems work as intended in the rapidly changing environments in which they must reliably collect evidence and investigative intelligence. Sometimes, this work has led to surprising observations about real-world surveillance systems. For example, in 1994, I discovered weaknesses in the NSA's "Clipper" key escrow encryption system that led to that system's abandonment before it was widely deployed. More recently, my graduate students and I found previously undiscovered vulnerabilities in analog telephone wiretaps used by law enforcement, and we identified ways for law enforcement agencies to harden their CALEA intercept systems against a variety of surveillance countermeasures.

There is perhaps no more ubiquitous symbol of our highly connected society than the cellular telephone. Over the course of only a few short decades, mobile communication devices have evolved from being little more than an expensive curiosity for the wealthy into a basic necessity for most Americans,

transforming the way we communicate with one another, do business, and obtain and manage the increasing volume of information that is available to us. According to recent estimates, there are today more than 285 million active wireless subscriber accounts in the United States. Many households now forgo traditional “landline” telephone service, opting instead for cellular phones carried by each family member. Wireless carriers have strained to keep up with the explosive demand for cellular service, in many areas deploying new infrastructure (most visibly cellular antenna towers) as quickly as they can find places to put it.

As difficult as it may be to imagine modern life without the cell phone, it is sometimes easy to forget how rapidly the technology has come about and how quickly new laboratory ideas in wireless communication can advance into the products and services that we take for granted. Over the last 25 years the mobile telephone has transformed from an analog voice-only service (originally available in only a few markets) into a high-bandwidth, always-on Internet access portal. “Smartphones”, such as the latest iPhones and Android devices, act not just as voice telephones but as personal digital organizers, music players, cameras, email readers, and personal computers, in a package that fits in our pocket. We now carry our phones with us wherever we go, and we expect them to have service wherever we happen to be.

Many of the most important and innovative new applications and services that run on mobile devices take advantage of the ability to quickly and

automatically detect the user's location to provide location-specific information and advice. At the same time, cellular providers calculate where phones in their networks are located (and how they move) to manage various network functions and to plan where new infrastructure is required.

2. Wireless Location Technologies

Unlike conventional wireline telephones, cellular telephones use radio to communicate between the users' handsets and the telephone network. Cellular service providers maintain networks of radio base stations (also called "cell sites") spread throughout their geographic coverage areas. Each base station is responsible for making connections between the regular telephone network and nearby cell phones when they make or receive calls. Cell phones periodically identify themselves to the nearest base station (that with the strongest radio signal) as they move about the coverage area. If a phone moves away from the base station with which it started a call and nearer to a different base station, the call is "handed off" between base stations without interruption. Phones will generally work any time they are within radio range of at least one base station, which allows users to use their phone at any location in their provider's geographic coverage area.

There are two different technological approaches for calculating the location of a cell phone. In one approach, the user's phone calculates its own location

using special GPS satellite receiver hardware built in to the handset. In the other, the cellular system calculates the location of the phones that are active in the network, using the normal cellular radio interfaces and without explicit assistance from the users' devices.

2.1 Handset-based GPS

For end-user applications that run on the telephone itself, the most prominent location technology is GPS. In GPS location, a user's phone contains special hardware that receives signals from a constellation of global position satellites. This allows a phone handset to calculate its latitude and longitude whenever it is in range of the satellites. GPS technology can achieve very high spatial resolution (typically within ten meters). In the latest phone models that incorporate the required hardware, GPS location features are integrated into applications for mapping, street directions, and to obtain information about local services and merchants.

Whether or not the calculated GPS location of a handset is sent to the network (or any other third party) depends on the application software that the phone is running. Some applications, as a matter of course, may periodically transmit their location to external services. For example, a mapping application might send its current GPS-calculated location to a network-based service in order to discover, say, the locations of nearby restaurants. Network-based services that

make use of a phone's GPS location might be offered by the cellular carrier or by a third party, internet-base entity.

Unfortunately, GPS, for all its promise, has a number of fundamental limitations. It relies on special hardware in the phone (particularly a GPS receiver chip) that is currently included only in the latest handset models and that generally is enabled for location tracking only when the phone user is explicitly using it to run a location-based application on the phone. Perhaps most importantly, it works reliably only outdoors, when the handset is in “view” of several GPS satellites in the sky above.

2.2 Network-based location

GPS is only one technology for cell location, and while it is the most visible to the end user, GPS is neither the most pervasive nor the most generally applicable phone location system, especially in the surveillance context. More ubiquitous are techniques that (unlike GPS) do not depend on satellites or special hardware in the handset but rather on data collected and analyzed at the cellular providers' towers and base stations. These “network-based” location techniques can give the position of virtually every handset active in the network at all times, regardless of whether the mobile device is equipped with a GPS chip and without the explicit knowledge or active cooperation of the phone user.

The precision with which a handset can be located by network-based (non-GPS) approaches depends on a range of factors, but has been steadily improving as technology has advanced and as new infrastructure is deployed in cellular networks. Under some circumstances, the latest generation of this technology permits the network to calculate users' locations with a precision that approaches that of GPS.

Network-based location techniques work by exploiting the cellular radio infrastructure that communicates between the network and the users' phones. All cellular systems have an extensive network of base stations ("towers") spread throughout their areas of service such that a cell phone in any locations in the coverage area is within radio range of at least one base station. This arrangement essentially divides the carrier's coverage area into a mosaic of local "sectors", each served by an antenna at the nearest base station. Network based location enables a cellular provider to identify the sector in which a user's phone is located, and, in some cases, to pinpoint their location within a sector.

2.2.1 Sector identification

At the most basic level, cellular providers record the identity of the particular base station (or sector) with which the phone was communicating every time it makes or receives a call and when it moves from one sector to another. How precisely this information by itself allows a phone to be located depends on the

size of the sector; phones in smaller sectors can be located with greater accuracy than those in larger sectors.

Historically, in the first cellular systems, the base stations were generally placed as far apart from one another as possible (to make the sectors as large as possible) while still providing adequate radio coverage across the area terrain. In early cellular systems, a sector might have covered an area several miles or more in diameter (and in sparsely populated, rural areas, this may still be true today). But as cellular phones have become more popular and users expect their devices to do more and to work in more locations, the size of the “typical” cell sector has been steadily shrinking.

The reason behind this trend toward smaller cell sectors is the explosive growth in the popularity of wireless technology itself. A sector can handle only a limited number of simultaneous call connections given the amount of radio spectrum “bandwidth” allocated to the wireless carrier. As the density of cellular users grows in a given area, the only way for a carrier to accommodate more customers is to divide the coverage area into smaller and smaller sectors, each served by its own base station and antenna. New services such as 3G Internet create similar pressure on the available spectrum bandwidth, usually requiring, again, that the geographic size of sectors be made smaller and smaller. At the same time, users increasingly rely on their mobile devices to work wherever they happen to be, indoors and out, on the street, in offices and residences, even in basements and elevators. The only

way to make service more reliable in more places under varying radio conditions is to add base stations that cover “dead spots”. This reduces the size of a sector's coverage area even further.

As a result, the number of cellular base stations has been growing steadily, with a corresponding decrease in the geographic area served by each. According to the most recent Cellular Telecommunications Industry Association (CTIA) study, there are more than three times as many cellular base stations today as there were ten years ago. Indeed, this trend has been accelerating in recent years, with the deployment of the latest generation of smaller and smaller-scale cellular base stations (called, variously, “microcells”, “picocells” and “femtocells”) designed to serve very small areas, such as particular floors of buildings or even individual homes and offices.

The effect of this trend toward smaller sectors is that knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location to within a relatively small geographic area. In relatively unpopulated areas with open terrain, this may be an area miles in diameter. But In urban areas and other environments that use microcells, this area can be quite small indeed, sometimes effectively identifying individual floors and rooms within buildings.

2.2.2 *Enhanced location with time- and angle- of arrival*

The decreasing size of cell sectors is not the only factor making network-based location more accurate. New technology allows cellular network providers to locate not just the sector in which the users' wireless device is located, but its position *within* the sector. By correlating the precise time and angle at which a given device's signal arrives at multiple sector base stations, it has become practical for a network operator to pinpoint a phone's latitude and longitude at a level of accuracy that can approach that of GPS.

A variety of “off-the-shelf” products and system upgrades have recently become available to cellular providers that use enhanced time- and/or angle-of arrival calculations to collect precise location information about users' devices as they move around the network. Current commercially available versions of this technology can pinpoint a phone's location to an accuracy of within 50 meters or less under many circumstances, and emerging versions of the technology can increase accuracy even beyond that. This is accomplished without special hardware is required on the users' phones, and accurate locations can be tracked in this way even when no calls are being made or received, as long as the user's phone is turned on and is within the coverage area. (Whether locations are routinely tracked and recorded at times other than when calls are made or received depends on the policy of the particular carrier).

Although these enhanced location technologies are not yet universally available in every network, wireless carriers are deploying them because they provide information that is extremely valuable in managing their networks and businesses. By tracking more precisely where each mobile device is located within a sector (and the direction it is moving), a carrier can better identify where new infrastructure is required, where old infrastructure is redundant, and how and where their customers use different wireless services.

While each carrier has its own data collection and retention practices, carriers typically create “call detail records” that include the most accurate location information available to them. Historically, before more advanced location techniques were available, carrier call detail records typically included only the cell sector or base station identifier that handled the call. As discussed in the previous section, the base station or sector identifier now carries with it more locational precision than it once did. But as even more precise location information becomes available, these records can now also include the customer’s latitude and longitude along with the sector ID stored in cellular carrier databases. Some carriers also store frequently updated, highly precise, location information not just when calls are made or received, but about every device as it moves about the networks. Maintaining such detailed records about the locations of phones as they move from place to place makes good engineering sense, and we should expect this trend to continue as part of the natural progression of technology. Once the infrastructure to collect it is installed, the cost of collecting and storing high resolution location data about

every customer is relatively small, and such information is extraordinarily valuable for network management, marketing, and developing new services.

3. Cell Phone Location and Law Enforcement Surveillance

As noted above, even on networks that do not employ time-of-arrival or angle-of-arrival location enhancements, the sector location by itself identifies the location of a surveillance target with increasing specificity as cellular sectors become smaller and smaller and as microcells, picocells, and femtocells are deployed to provide denser coverage. In legacy systems or in rural areas, a sector ID might currently specify only a radius of several miles, while in a dense urban environment with microcells, it could identify a floor or even a room within a building. How precise sector identity is depends on the particular location of the target and on the layout of the particular carrier's network.

Most carriers' systems use a variety of large and small sector configurations. A mobile user, in the course of his or her daily movements, will periodically move in and out of large and small sectors. Even if the network only records cell tower data, the precision of that data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise, and neither the user nor the carrier will be able to predict whether the next data location collected will be relatively more or less

precise. For a typical user, over time, some of that data will likely have locational precision similar to that of GPS.

As cellular carriers roll out better location technologies in the course of their business, the location information sent to law enforcement (as transmitted from the carrier's call database in (near) real time in response to a wiretap order) is becoming become more and more precise. The current base station or sector ID paradigm is becoming less important to carriers, and as networks improve, sector data is increasingly being linked to or supplanted by an accurately calculated latitude and longitude of the customers' handsets.

In the past, when cell sectors were widely spaced and before the availability of the enhanced network-based location technologies now being deployed by wireless carriers, it may have technically sound to distinguish between location based on the cellular network (at presumably low accuracy) and that based on GPS (at high accuracy). Today, however, this distinction is increasingly obsolete, and as cellular networking technology evolves, it is likely to become effectively meaningless. As microcell technology and enhanced location techniques becomes more widely deployed in cellular networks, the information revealed by through the cell sector identifier pinpoints, under many circumstances, a user's location to a degree once possible only with dedicated GPS tracking devices. It is no longer valid to assume that the cell sector recorded by the network will give only an approximate indication of a user's location. The gap between the locational precision in today's cellular

call detail records and that of a GPS tracker is closing, especially as carriers incorporate the latest technologies into their networks.

As the precision provided by cellular network-based location approaches that of GPS-based tracking technology, cellular location tracking can have significant advantages for law enforcement surveillance operations compared with traditional GPS trackers. New and emerging cell location techniques can work indoors and in places not typically accessible to GPS receivers. Cell phone location information is quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the subject. And the “tracking device” is now a benign object already carried by the target -- his or her own telephone.