Location Based Services
Bug or Feature?

Michael Pridat

July 2007

Term paper
Ruhr-Universität Bochum

Chair for Communication Security
Prof. Dr.-Ing. Christof Paar

Contents

List of Figures

List of Tables

1 Introduction

In our technology-inspired society nobody wants or can live without a mobile phone nowadays. Nearly everybody is using or owns a mobile phone. Wherever people go their mobile phone is with them day-to-day. The current mobile phone generation offers three or more mega pixel cameras, large displays, different data exchange methods, sensitive microphones and memory witch can simply be upgraded to several gigabyte. Thus all technical requirements for an abuse are available. Conversations and calls can be recorded, pictures can be taken without raising suspicion. By activating the mobile phone from any remote location and using it as an eavesdropping tool it could be done more simply. Precisely because the mobile phone is always near by and connecting itself with the strongest base station, an aggressor only needs to analyze the base station protocols for creating specific movement profiles.

In this term paper two topics are discussed in detail which are referenced to location-based services. In Chapter 2 the possibilities for using mobile phones as eavesdropping tools are described. What's possible and how easy is it? Is the mobile phone currently used by government or other organizations as an eavesdropping tool? Furthermore the complexity of using a mobile phone as a bug will be discussed.

Chapter 3 deals with **l**ocation-**b**ased **s**ervices (LBS) and their usage. The question how easy it can be to locate a mobile phone using LBS provider in the internet will be answered. Additionally techniques which are commonly used for localization will be described. Finally, there is a comparison of LBS providers to explain how they work and which security problems exist which will be concluded in Chapter 3.2. All results are combined and compared in Chapter 4

2 Can a mobile phone act as a bug?

This chapter the question if a usual mobile phone can be used as a bug is discussed. Is it possible to turn on the microphone of a mobile phone without any notice of the owner? If this is possible then question occurs if this technique can be used for other functions of mobile phones e.g. camera as well?

First of all the three major security vulnerabilities of a mobile phone are listed:

- Vulnerability to monitoring of your conversations while using the phone.
- Vulnerability of your phone being switched into a microphone to monitor conversations in the vicinity of your phone while the phone is inactive.
- Vulnerability to "cloning", or the use of your phone number by others to make calls that are charged to your account.

This term paper will only describe the second vulnerability aspect. Before discussing the second vulnerability, here is a short insight on how mobile phones and base station cooperate.

The mobile phone send radio frequency transmissions through the air on two distinct channels, one for voice communications and the other for control signals. When a mobile telephone is first swiched on, it emits a control signal that identifies itself to a cell site (base station) by broadcasting its mobile identification number (MIN) and electronic serial number (ESN), commonly known as the "pair". When the base station receives the pair signal, it determines if the requester is a legitimate registered user by comparing the requester's pair to a cellular subscriber list. Once the mobile phone's pair has been recognized, the cell site emits a control signal to permit the subscriber to place calls at will. This process, known as anonymous registration, is carried out each time the phone is switched on or picked up by a new cell site. [1]

Are there any references that anybody has already used mobile phones as bugs? According to press reports the **F**ederal **B**ereau of **I**nvestigation (FBI) has been successful in using a mobile phone as a bug. [2] FBI is not willing to disclose the used technique, but due to security experts the so called **o**ver-**t**he-**a**ir programming[1] (OTA) has probably been used for this. With OTA automatic

[1]The OTA mechanism requires an existing software and hardware of the target device to support the feature, namely the receipt and installation of new software received via the wireless network from the provider.

updates of mobile phone firmware or wireless assignment of defined matters (like WAP[2] or MMS[3] settings) are possible from afar through the mobile network for compatible end devices. Through OTA new software is transferred to the phone, installed, and put into use. It is often necessary to turn the phone off and back on for the new programming to take effect, therefore many phones will automatically perform this action. [3]

What has been meant as special convenience from manufacturer side for users, turns out to be a big security vulnerability according to opinion of many data security people. Originally this wireless programming technique should avoid sending in the mobile phone for firmware updates and therefore being spared at that time from their users. At the same time this technique offers the chance to replace the phone software unnoticed.

2.1 Mobile phone micro as an eavesdropping tool

The FBI uses the potential of recent mobile phone models to eavesdrop suspects through their cell phone even though the phone seems to be switched off. The technique was approved by the U.S. Department of Justice officials for use against members of a New York organized crime family who were wary of conventional surveillance techniques such as tailing a suspect or wiretapping him. [2] A recent court confirmed [4] it to be legal that the FBI has the ability to activate, access and control a cell phone from a remote location and turn its microphone into a listening device that transmits to an FBI listening post. [5]

The FBI converted the *Nextel* mobile phones of two alleged New York mobsters into "roving bugs" – microphones that relayed conversations when the phones seemed to be inactive.

2.2 Requirements

In the previous part the FBI technique called "roving bug" for eavesdropping any people was introduced. Using the mobile phone as a bug seems to be able. The requirements, necessary for this "roving bug" technique, are:

1. It seems that only certain mobile phones can be used for eavesdropping. This is the matter if they can be reprogrammed over the air, using methods meant for delivering upgrades (Firmware updates) and maintenance.

[2]Short for the **W**ireless **A**pplication **P**rotocol, a secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones, pagers, two-way radios, smartphones and communicators.

[3]**M**ultimedia **M**essage **S**ervice is a store-and-forward method of transmitting graphics, video clips, sound files and short text messages over wireless networks using the WAP protocol

Examples for such mobile phones are *Motorola Razr*[4] and *Samsung 900*[5] series mobile phones.

2. The second requirement is not mandatory. A phone which is in stand by mode even though it is switched off is required. This can be easily identified, because on these phones e.g. an alarm clock function is still working even though the phone is switched off. Such as the alarm clock function, spyware or other "bad" programs can develop its full effect as well on this stand by mode.

2.3 Realization

For the mobile phone as an eavesdropping tool the OTA update function is not used to transfer firmware or other official software but rather "special" software which can offer one of the following features.

- The standard software user interface is manipulated or overwritten in a way that phone calls which are done over the infiltrated program are not shown.
- This special software is able to accept an incoming connection (e.g. a call from a certain number) without showing this on the mobile phones user interface. This is possible as long as no connection is existing at the same time.
- If the phone gets switched off the software only pretends this (e.g. turning off the display). Incoming or outgoing connections are still possible.
- Even though the mobile phone gets switched off it is in a standby comparable status, like mentioned above. The special software is operating in the background like the alarm clock function. Connection establishment or answering a call is in this status already possible.
- It is also possible to deposit an audio recording in internal buffer of the phone, as all mobile phones have big memories by now, and send these recordings in batches.

For all mentioned points not only connection establishment of the telephone lines needs to be considered. Also multi media functions like bluetooth can be used for data transfer. Over all the victim does not recognize the established connection.

[4] http://www.motorola.com
[5] http://wireless.samsung.de/type_phone_fax_gsm.asp

3 Mobile phone localization for everyone

The third chapter contains localization techniques and how they are detecting mobile phones. At the end of this part a selection of internet offers (e.g. of detecting your kids mobile phone) is listed and compared. Wherever mobile phone users stay, they are permanent accessable. That's the matter why they can also be located everywhere, if their phone is switched on.

As a result of this, many new options arise:

- Users subscribe search functions for friends or their children
- Users can be sent information on the cell phone about shopping facilities or restaurants referring to their surrounding area
- Companies can monitor their car pool and field manager at the PC

All these functions are so called location-based services (LBS). Location-based services are mobile services offered by mobile phone networks as a way to send customer advertising and other information to mobile phone subscribers based on their current location, time or personal data.

Capturing of the actual position becomes more questionable, if people are located without their knowledge or without their agreement. That is technically possible, but formally illegal.

3.1 Locating of mobile phones

For a long time locating in cell based wireless networks was quite inaccurate. Only the current used cell was specified. But through a regulation of US "**F**ederal **C**ommunications **C**ommission" (FCC)[6] the development of more exact procedures was raised. Point of origin were the geographical conditions of the USA.

[6]The FCC is assigned with regulating all non-Federal Government use of the radio spectrum (including radio and television broadcasting), and all interstate telecommunications (wire, satellite and cable) as well as all international communications that originate or terminate in the United States.

Sometimes people who had a heavy accident or an emergency case did not know where they are, because of the wide areas or very long Highways. During an emergency call they could not explain their actual position. For this reason wireless network providers were forced to develop so-called "Enhanced 911" - services (E-911)[7], until October 2001. Through this service an automatically position data transmission with a maximum deviation of 125 meters should be ensured if the emergency call is done by mobile phone.

Since then, different localization technologies have been developed which should guarantee that the exact location can be found. The different types will be discussed below.

3.1.1 The locating technology

The most mobile localization technologies are based on the **G**lobal **S**ystem for **M**obile Communication (GSM[8]).

Basically there are two different kinds of localization:

- Absolute: The absolute localization does not require any information about previous positions.
- Relative: The second technology can measure any position change autonomously from the environment and the absolute localization can be added.

In the remainder the absolute technologies, which are used by GSM are described.

For detecting a point in relation to other known reference points, two basic methods are used. Trilateration and Triangulation. During the absolute localization the position is determined by measuring the distance (known as trilateration) or angle (triangulation) to known reference points.

[7]Enhanced 911 or E911 service is a North American telephone network (NANP) feature of the 911 emergency-calling system that automatically associates a physical address with the calling party's telephone number.

[8]GSM: originally from Groupe Spécial Mobile is the most popular digital transmission standard for mobile phones in the world.

Trilateration and Triangulation

As already mentioned above **Trilateration** uses the known locations of two reference points and the measured distance between the subject and each reference point. For two and three dimensional localization three reference points are needed at least. In practice the accuracy can be increased by using further points.

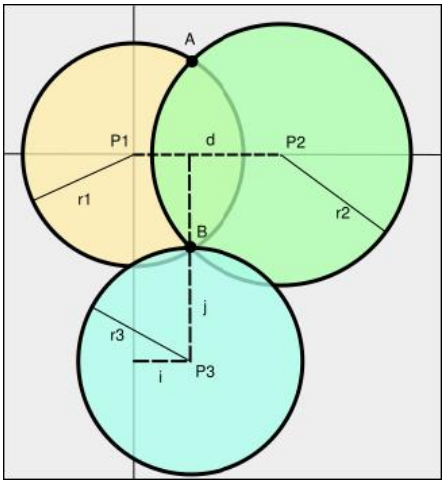


Figure 1: Trilateration
[6]

The location of the point (B) relative to the reference points (P1), (P2), and (P3) on a two dimensional plane is calculated. Measuring the distance *r1* narrows the possible position down to a circle. Next, measuring the distance *r2* narrows it down to two points, (A) and (B). A third measurement, the distance *r3*, gives the coordinates at (B). A fourth measurement can be made to reduce errors. [6]

Triangulation, which uses angle measurements (together with at least one known distance) to calculate the subject's location, is used in cellular communications to pinpoint the geographic position of a user.

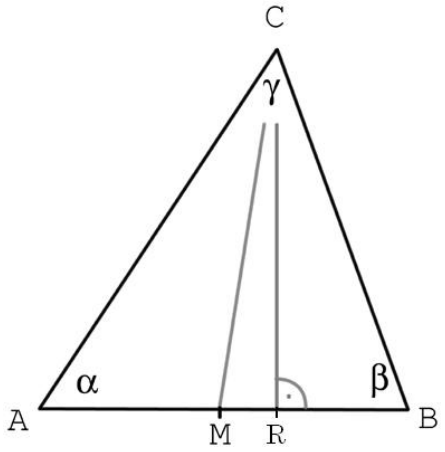


Figure 2: Triangulation
[7]

Currently the location of the point (C) is searched. The position can be calculated using two reference points (A) and (B) witch positions and angles α and β are known already. The distance AB is known as well. The unknown location of (C) can be calculated by using the angles via law of sines and law of cosines. For three dimensional localization at least three angles are required for calculation.

- α, β and the distance AB are already known
- C can be calculated by using the distance RC or MC:

RC: Position of C can be calculated using law of sines and law of cosines

$$\gamma = 180^\circ - \alpha - \beta \qquad \frac{\sin\alpha}{BC} = \frac{\sin\beta}{AC} = \frac{\sin\gamma}{AB}$$

Now it is possible to calculate AC and BC

$$AC = \frac{AB \cdot \sin\beta}{\sin\gamma} \qquad BC = \frac{AB \cdot \sin\alpha}{\sin\gamma}$$

Last step is to calculate RC via

$$RC = AC \cdot \sin\alpha \quad or \quad RC = BC \cdot \sin\beta$$

MC: MC can be calculated using the Pythagorean theorem

$$MR = AM - RB = \left(\frac{AB}{2}\right) - (BC \cdot \cos\beta) \qquad MC = \sqrt{MR^2 + RC^2}$$

In some situations (for example in an emergency case like mentioned above) it might be necessary for people to be localized. This can be achieved by triangulation if the person carries a mobile phone with him/her. The USA 911 system automatically report the telephone number and location of 911 calls made from mobile phones, a capability called Enhanced 911, or E911. But triangulation apparatus can be confused by the reflection of signals from objects such as large steel-frame buildings, water towers, communications towers and other obstructions. For this reason, at least two independent triangulation determinations should be made to confirm the position of a mobile phone or other radio transmitter [8].

The most popular methods of position location capabilities being built into cellular networks will be listed subsequently. Starting with network-based systems (TDOA & TOA, AOA), subsequently handset-based methods (E-OTD) are presented.

Time Difference of Arrival (TDOA)

One of the more simple network-based methods, TDOA, uses the time it takes for a signal to travel as an indirect method of calculating distance. With a minimum of three base stations receiving a signal from a mobile phone, the difference in time it takes for the signal to reach each tower can be used to triangulate the position of the mobile unit. To achieve accurate positioning, the base stations need to be precisely synchronized in time.

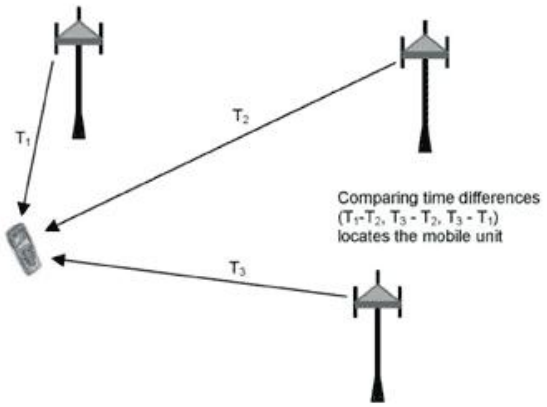


Figure 3: Time Difference of Arrival
[9]

Time of Arrival (TOA)

Similar to the TDOA technique, this technology only differs in the fact that it uses the absolute time of arrival at a certain base station rather than the difference between two or more stations. The distance can be directly calculated from the time of arrival because signals travel with a known velocity. Time of arrival data from two base stations will narrow a position to two points and data from a third base station is required to resolve the precise position. As with TDOA, synchronization of the network base stations is important. This synchronization can be done in different ways:

- With exact synchronous watches on both sides
- With two signals which have different spreading speed. Distance to a lightning strike can be measured that way (speed of light and sound velocity).
- Via measurement to a second reference point

Inaccuracy in the timing synchronization translates directly to an imprecise location.

Enhanced Observed Time Difference-Technology (E-OTD)

This method includes new technology in a mobile phone to assist in locating the base station in a network. This is similar to network based TDOA, but in an E-OTD system the position is estimated by the mobile phone, not by the base station because they are asynchronous. One implementation of this method has the mobile phone reporting back measured times from at least three base stations. The measured times are combined with timing data from various points in the network in order to determine the location of the mobile phone [9]

Angle of Arrival (AOA)

This method uses multiple antennas at a base station to determine the incident angle of an arriving signal. If a mobile phone is transmitting a signal within line-of-sight, the antenna array can determine what direction the signal is coming from. A second base station with the same technology would then also locate the handset and compare it with data from the first base station to pinpoint the caller's location. AOA systems must be designed to account for multipath signals (those that bounce off other objects), since they may confuse the location of the mobile phone. Also, installing and aligning antenna arrays on base stations can be a sensitive and costly process.

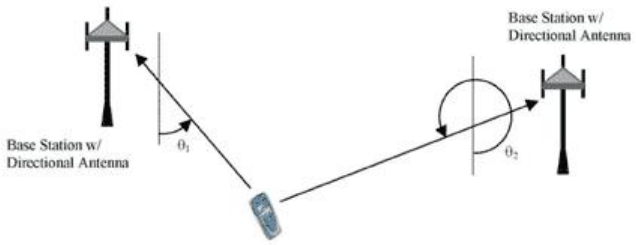


Figure 4: Angle Of Arrival
[9]

Cell of Origin (COO)

To be complete the easiest and widespreaded but inexactest method of positioning needs to be named as well. It is still used in germany cellular networks. The network based Cell of Origin-Technology is a positioning technique for finding a caller's cell location. Cell means the basic geographical coverage unit of a mobile phone system. Each base station represents a cell in its area. For COO positioning, the location of the base station is ascertained and considered to be the location of the caller. COO can very quickly identify the location (generally in about three seconds) and does not require equipment or network upgrades. But COO is a variable and not a very precise locater, depending on the number of base stations in the search area. In urban areas smaller cells with more base stations are used. Therefore the localization is more exact then in rural areas. [10]

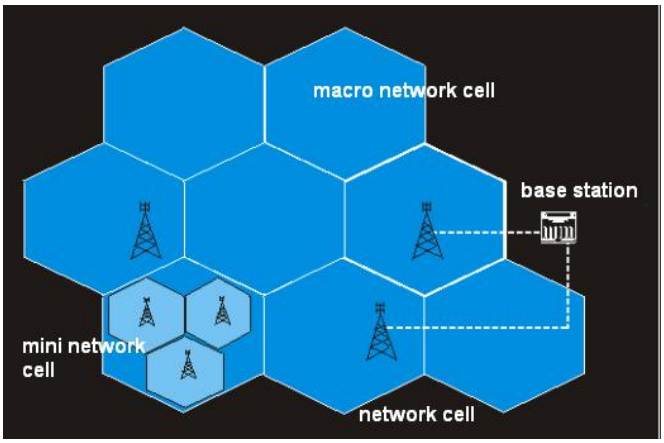


Figure 5: Network cell
[11]

O_2 (a mobile phone provider in Germany [12]) uses COO for their homezone technique. As long as the customer stay in his homezone area, his calls are cheaper than outside.

When precision is important COO is often used in conjunction with some other technology, such as above described Time of Arrival (TOA).

3.1.2 Accuracy

The location information is generally much more accurate in urban areas than in rural areas. [13]

- URBAN AREAS: Built up areas and cities such as Hamburg, Berlin or the Ruhr-area can expect accuracy between 50m to 400m.
- SUBURBAN AREAS: Suburban areas vary between 450m and 2km.
- RURAL AREAS: Due to the sparse nature of the operator base stations in rural areas the accuracy can vary from 1.5km to 9km.

Furthermore the accuracy of the location information depends on the used localization technique. The accuracy of COO ranges between 150 meters and 30 kilometers - dependent on the cellsize mentioned above. With TOA technique the accuracy can be enhanced to 50-200m. With TDoA technique it is even 50m to 100m precise.

3.2 LBS Provider comparison

In this chapter different LBS provider and their accuracy and registration requirements are tested. Unfortunately the LBS provider keep their used technology secret. They indicate only the standard accuracy between 100m and 800m on their homepage. The following LBS provider are described:

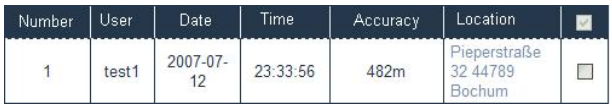
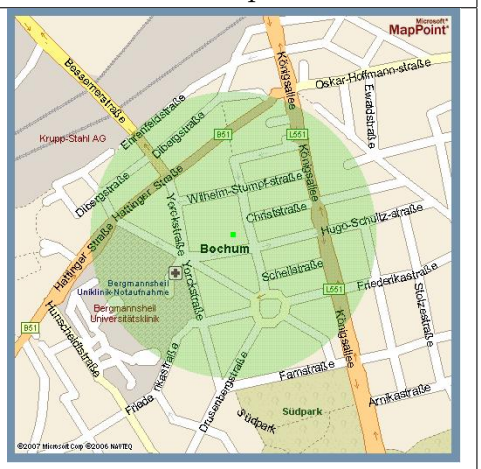
Provider	Price (GSM)	Registration	Safety	Free localizations	Extras
www.corscience.de	49ct	Yes	SMS for activation	4	Google Earth Link / Interval localization
www.picosweb.de	49ct	Yes	SMS for activation / SMS Reply for confirmation	1	–
www.trackyourkid.de	35ct–1€	Yes	SMS for activation / SMS Reply for confirmation	0–20	up to 5 numbers for localization can be stored
www.via-ferrata.de (based on picos)	99ct	Yes	SMS for activation / SMS Reply for confirmation	1	–
www.handy-ortung.5zu7.de (based on picos)	49ct	Yes	SMS for activation / SMS Reply for confirmation	1	–

Table 1: Different LBS provider

All tested LBS provider have a common security problem. The customer simply needs to activate his mobile phone at his mobile network operator (*vodafone*, *eplus*, O_2) via SMS[9]. Sometimes he gets a confirmation via SMS for activating the LBS function. Once this function is activated further localization trials effects unnoticed. No other information SMS or something else is submitted during localization. It seems to be guaranteed that no foreign mobile phone can be located. Indeed no one is assured that a friend, mate, family member, stranger etc. uses this mobile phone sending an activation SMS. From then he can get information about the habitation without any knowledge of the mobile phones owner.

In order to get more information about the used technology and registration requirements I announced myself at Corscience GmbH & Co. KG [14], jackMobile GmbH [15] and INTERVISTA AG [16]. In all three cases the free localizations were performed. All three provider localization results are completely comparable. One of these results is depicted below.

[9] In Germany only *vodafone*, *eplus* and O_2 are supporting the activation via SMS. For activating and locating T-Mobile phones, the owner has to permit *T-Mobile* (in writing form) to relay the position data

Location	Map
	

Number	User	Date	Time	Accuracy	Location	
1	test1	2007-07-12	23:33:56	482m	Pieperstraße 32 44789 Bochum	

Table 2: Corscience localization result
[14]

All tested LBS provider prepared the information they get from the network provider in a special way. Some display further information according to the current located position like streets which are close by or latitude and longitude. But the original data is always identical.

The following conclusions can be done using the comparison of localization results:

- German network provider are using COO for localization. The result of all taken LBS provider are alike. Only the output format and additional offers (SMS, email, text, map, etc.) differ from LBS provider to LBS provider.
- The located position is given by the current used base station. The base station is shown at the maps.
- The accuracy in urban areas is still higher than in rural areas, as expected.
- Details of surroundings (e.g. street and street number) are often imprecise and lead to confusion.
- An accuracy of 125 meters like in the USA cannot be attained in Germany. The average accuracy of the test series were 300 meters.

At the end there is still one question left. Is the location data only accessible for the people which it is intended for?

4 Conclusion

This written term paper exemplifies two miscellaneous themes which are strongly connected to location based services. Chapter 2 describes how wiretapping via mobile phones can probably be done and which preconditions need to be created. After analyzing different newspapers and online reports, wiretapping through mobile phones seems to be possible and might be done by public authorities already. The question that occurs in this context is: "If public authorities can use such a mechanism, how big is the chance that it is open for other people as well?" But, all introduced mechanisms have one essential requirement in common, they need electricity. Thus, the only advice which is useful as counteraction, is to take out the rechargeable battery of the phone when sensitive information needs to be talked about.

There are also positive applications. With OTA the firmware of a mobile phone can be changed, which gives new perspectives to cautious employers as well. When entering the company building the firmware of employees mobile phones can be modified. Critical functions such as camera are switched off or network settings for WLan and Bluetooth are changed according to company's safety regulations. When leaving the company all functions of mobile phone are available again. But therewith only one of many security gaps is closed: Visitors will probably not allow access to their own mobile phones and even for insider jobs human being as data medium cannot be excluded as risk factor. [17]

The second theme which has been discussed in Chapter 3 relates to different localization techniques. How can they be used for permanent monitoring of our actual position? These techniques for exact positioning are described more closely. At the end a field test with several LBS-provider was made in order to find out how precise and unproblematic people can be located. The techniques clearly demonstrate the localization problem. Everyone can locate a foreign mobile phone using the LBS provider described above. There is also just one useful advice against locating and creating movement profiles. If possible you have to change frequently your mobile phone or SIM-Card with friends, colleagues or intimates. That way the allocation becomes more difficult. Switch your mobile off and remove the rechargeable battery if you can not do the above method.

Bibliography

[1] U.S. Department of Commerce/Office of Security. Employees' guide to security responsibilities, 2001.
http://www.wrc.noaa.gov/wrso/security_guide/cellular.htm.

[2] Declan McCullagh and Anne Broache. FBI taps cell phone mic as eavesdropping tool. 2006.
http://news.com.com/FBI+taps+cell+phone+mic+as+eavesdropping+tool/2100-1029_3-6140191.html.

[3] Wikipedia. Over-the-air programming, 2007.
http://en.wikipedia.org/wiki/Over-the-air_programming.

[4] District Judge [United States District Court] Lewis A. Kaplan, 2006.
http://www.politechbot.com/docs/fbi.ardito.roving.bug.opinion.120106.txt.

[5] Vic Walter and Krista Kjellman. Can you hear me now? 2006.
http://blogs.abcnews.com/theblotter/2006/12/can_you_hear_me.html.

[6] Wikipedia. Trilateration, 2007.
http://en.wikipedia.org/wiki/Trilateration.

[7] Florian Nehonsky. Entfernungsmessung im Weltall, 1998/1999.
http://pluslucis.univie.ac.at/FBA/FBA99/Neho.

[8] SearchNetworking.com. Triangulation, 2001.
http://searchnetworking.techtarget.com/sDefinition/0,290660,sid7_gci753924,00.html.

[9] Unstrung.com. Wireless Location Technologies. 2002.
http://www.unstrung.com/document.asp?doc_id=15069&page_number=1.

[10] Carsten Schulte and Christoffer Riemer. Handy-Ortung und GPS-Ortung, 2005.
http://www.iwi.uni-hannover.de/lv/ucc_ws04_05/riemer/frame_haupt.htm.

[11] ZDNET. Funkzelle.
http://www.zdnet.de/glossar/0,39029897,70009550p-39001588q,00.htm.

[12] O_2 Germany.
http://www.o2online.de.

[13] MobileLocate.co.uk. Accuracy, 2004.
`http://www.mobilelocate.co.uk/accuracy.htm`.

[14] CORSCIENCE GmbH & Co. KG.
`http://www.avetana.de/cocoon/ortung/login-corscience.de`.

[15] jackMobile GmbH.
`http://www.trackyourkid.de/`.

[16] INTERVISTA AG.
`www.picosweb.de`.

[17] Sascha Koesch, Fee Magdanz and Robert Stadler. Handy-Fernsteuerung gegen Mobil-Schnueffler. 2006.
`http://www.spiegel.de/netzwelt/mobil/0,1518,454709,00.html`.