

Cellular Telephones vs. Privacy

The same technology that has led to the current popularity of cellular telephones has also made cellular telephone systems all the more susceptible to unauthorized interception. A common misconception held by many cellular telephone users today is that the advanced level of technical sophistication employed in cellular telephone systems correspondingly reduces vulnerability to interception of their mobile telephone calls. They are greatly mistaken.

While the sophisticated complexities of the cellular telephone system may frustrate the efforts of casual radio monitoring curiosity seekers, they are a tremendous asset to the professional intercept operator. Not only do they facilitate monitoring the conversations of a specifically designated target, but the exchange over radio waves of digital data between the cellular telephone unit and the main cellular telephone system computer provides a wealth of information to the skilled intercept operator.

Few cellular telephone users are aware that once their mobile or portable cellular telephones are turned on there is a continual exchange of information between their units and the main computer. This information exchange occurs every few minutes and is the means by which the cellular telephone informs the computer of who it belongs to, where it is located, and that it is ready to receive or initiate a call for the unwary user, there is no observable indication that this data exchange is taking place even though the cellular telephone is not actually being used in a conversation. An example of just part of the information being exchanged will illustrate its importance to the intercept operator.

The Mobile Identification Number (MIN) is the standard ten digit telephone number of the cellular telephone. The cellular telephone frequently transmits its own telephone number to the cellular system computer to identify itself and disclose its location. If there is an incoming call for the cellular telephone, the system computer will know that it is available to receive the call and in which cellular cell coverage area it is located. The computer will then address that particular cellular telephone by its number. The cellular telephone also sends its own telephone number, as well as location determining information, when an outgoing call is placed. From the area code and first three digits of the telephone number, the intercept operator can quickly determine the geographical area in which the cellular telephone owner is a subscriber. This is called its home base.

Another means of determining the home base of the cellular telephone is through the System Identification Designator (SID), which is a 32 bit code that identifies the specific company, and its location, to which the user subscribes for cellular telephone service. Each individual company system throughout the world has its own unique identification code, and that code is programmed into the cellular telephone unit. This is how the cellular telephone companies know where to send the subscriber's bill. If a cellular telephone user from New York uses his unit in San Francisco, the automatic transmission of the System Identification Designator data will tell the San Francisco cellular telephone company exactly where to send the subscriber's bill in New York. It also tells the intercept operator the location of the user's home base.

For the intercept operator, the Electronic Serial Number (ESN) is of paramount importance. The Electronic Serial Number consists of a series of bits of information representing the unique identifying serial number of each individual cellular telephone. While the Mobile Identification Number and the System Identification Number can be changed with relative ease, the Electronic Serial Number is permanently programmed into the cellular telephone at the factory by the manufacturer. It is what identifies a single cellular telephone out of the millions distributed worldwide, and is as unique as a person's fingerprints.

Quite often, an intercept operator will simply program the monitoring equipment to activate upon receipt and recognition of an Electronic Serial Number rather than the Mobile Identification (telephone) Number. Should a targeted cellular telephone user change the Mobile Identification Number, or obtain service from another company, the intercept operator would immediately have the new Mobile Identification Number and the System Identification Designator information and simply update the programming of the monitoring equipment.

Once the intercept operator locks on to a specific cellular telephone it will respond to control instructions from the cellular system computer much the same as the cellular telephone being monitored. Whenever the cellular telephone is switched from one channel to another as it passes through a cell, or from one cell to another, the monitoring equipment will switch likewise to enable continuous, uninterrupted monitoring and recording throughout each and every conversation. The user's only defense is to exercise caution in what is discussed when using a cellular telephone.

But a good intercept operator can do more than simply acquire identification information and eavesdrop on sensitive cellular telephone conversations. Every cellular telephone consists of a radio transmitter and receiver. The transmitter emits a signal that the intercept operator can use to home in on and precisely locate the unsuspecting user. If the cellular telephone is installed in a vehicle, the signal it radiates--even when the cellular telephone is not in use- can be used to track the vehicle as it moves about. Cellular telephones often make excellent tracking transmitters.

Worse yet, cellular telephones, especially mobile units, can be used in assassination efforts. A miniature, relatively simple, preprogrammed digital dual-tone decoder circuit and a compact explosive, lethal gas, or incendiary device can easily be connected to a cellular telephone. Then days, weeks, or months later, the assassin simply calls the cellular telephone user. Once the assassin's intended target is using the cellular telephone, the assassin quickly dials the appropriate preprogrammed code. In less than half a second the code is detected and the lethal device activated. The assassin could conceivably originate the deadly call, and activate the device, from half-way around the world via an international direct-dial call.

Corporate executives, diplomats and government officials, defense contractors, business people, and celebrities are all subject to having their most confidential cellular telephone conversations monitored. For the competent intercept operator, one target is just as easy to monitor as the other. The Electronic Communications Privacy Act making unauthorized interception of cellular telephone conversations a crime is hardly a deterrent to most illegal intercept operators because it is almost impossible to detect their activities. They simply sit quietly in their hotel rooms or vehicles and monitor the air waves. Since their compact monitoring equipment is fully automatic, they do not even have to be present as sensitive cellular telephone conversations of their unsuspecting targets are being recorded.

Commercial and industrial espionage has become a multi-billion dollar a year business, and selective monitoring of cellular telephone conversations is one of the easiest, most expedient, cost effective means of acquiring sensitive information while incurring minimal risk of being discovered. Cellular telephone are wonderful devices, but the convenience and ease of operation they offer lull perhaps too many users into a false sense of security--a security that simply does not exist. Ask any intercept operator.