CellAntenna
SOLVING CELLULAR COMMUNICATION PROBLEMS WORLDWIDE

Answers to the NTIA
Questions and Comments on Cell Phones and Prisons

Prepared by Howard Melamed

CEO CellAntenna Corp. 06/08/2010

CellAntenna Corp currently performs jamming of communication (Signal Denial) and Cell Phone Controlling which the NTIA refers to as Managed Access. We have experience in these systems in actual customer locations around the world. Our capabilities and experience put us in a position to provide a response to the NTIA request. It should be noted however, that even though the NTIA had requested specific techniques, engineering methods etc., we believe that this would compromise our NDA's as well as national security. It is important to note therefore that my discussion will be limited in nature but should suffice. I urge the NTIA not to publish anyone's methods, techniques or engineering formula due to the concern for national security should this information be available in the wrong hands. Furthermore, any and all information published here will become readily available to inmates who are quite industrious and have access to PDA's with internet availability. With a lot of time on their hands, we have found that inmates have a way of figuring these things out.

Introduction

There are more than 2.5 million inmates in local and state correctional facilities. Almost all of these facilities have access to the cellular network, i.e. the use of cell phones, due to the proximity of the private sector cellular carrier services, and the FCC's instance on coverage within a licensed area. Often the cell towers are located within the facility itself where the government organization in an effort to mitigate the growing costs of penal administration rent tower space to the cell phone providers. In some cases, the institution themselves have installed repeaters to provide better coverage of cell phone communication, without examining the consequences.

Currently the cellular carriers have accepted no responsibility to prevent the use of cell phones by inmates. It has been our contention that the carriers have no interest in this for two reasons. 1) They are currently receiving substantial revenues from inmates that are easy customers that pay bills on time and offer no resistance to quality of service. 2) The cost of accepting this responsibility would involve billions of dollars. As I have always stated: The Carrier has the capability to stop cell phone communication inside most of the prisons in this country, but is not required to do so by the FCC.

Strategies and Tactics:

It has been our experience that there is no one complete system, or 'Black Box' that fits all situations and that can be relied upon for 100% removal of the problem. We believe that the need for multiple methods is required to provide the maximum removal of cell phone communication use by inmates. These techniques are currently touched upon by the NTIA, including Jamming, Cell Phone Control, used in conjunction with searches, shakedowns, metal detectors etc. By utilizing a strategy and multiple techniques, no one system can be defeated that would lead to a collapse of the whole systems. In other words, if we were to deploy jamming only, having the system attacked by the inmates through physical techniques, intelligent systems, or by compromising security personnel through bribes and payments, would defeat the system, leaving cell phone communication open again.

Similarly, in the use of Managed Access where a direct communication link is made to the carriers, whereby the system is managed outside of the security team, compromising the system is relatively easy either by paying off lower management tiered people within the carriers, or by the use of a small jammer that can be as easily obtained as the cell phone itself, attacking the Managed Access provider's system defeating the protection that it provided. It is important to note that it is this specific false sense of security that lies at the heart of the problem: No one system is 100% effective and a combination of several redundant controls need to be put into place. Jamming by itself is not a solution but rather one of the solutions needed to be combined with others.

Understanding this principle and one can understand our resistance to having any one product certified by any organization for use in a prison. We believe that all systems need to be engineered, and each prison requires a different solution. Our experience with D.C for example, where we were going to perform a jamming experiment for the Department of Corrections under an STA from the FCC, resulted in our determining that the area to be jammed at this demonstration had too high of a signal level that would make jamming safe. In different instances different methods need to be deployed. Therefore if a prison is located in a rural area, some solutions would be better than the city area and vice versa.

Answers to Specific questions asked by the NTIA:

1. Technologies or Approaches Jamming, Managed Access, and Detection

The characteristics are accurate, but need some revision regarding effectiveness and looking at them from a security standpoint.

We take an engineering approach when performing jamming in a prison setting. In some cases jamming simply cannot be safely accomplished. That is, if signal levels coming for towers are too high, the amount of jamming signal that will be needed will be hard to control. That is why one solution does not fit every case, and to properly suppress communication within a prison facility you must be able to supply all necessary systems under an engineering design.

Two type of managed access techniques exist. One is an on air system whereby communication with the cellular carriers is required and offered. The other is the off air system where no connection between the carriers and the managed access unit is required. Our term for the latter is Cell Phone Control (CPC). It is our belief that given the security aspect and the ability to compromise on air systems, the CPC is preferred. Cell Phone Control detects all cell phones in a target area individually, identifying their IMSI/IMEI ESN/MIN properties. Once detected the cell phones are then disconnected from the cellular network, or made inoperative by other means.

Another similar CPC system that we deploy is called Reactive Suppression. Each cell phone detected in a target area has its voice transmission suppressed rendering the call useless. This method does not interfere with RF communication, as we do not disconnect the call. We can also exclude certain cell phones from being suppressed.

It has been our experience that each prison requires customization and that there can be no 'black box' one size fits all solution. Factors in determining the system concepts include the size of the prison., its location to rural or city , the building materials, its security level (High, medium etc.) and the nature of the problem of cell phone communication (there can be circumstances that suppression of cell phones is simply not an issue)

All of our technologies that we deploy allow for technology refresh, that is, as new systems, protocols and frequencies become a threat to the prison institution, the methods to control them can be deployed within the same infrastructure.

The use of cell phones by anyone entering a facility is prohibited in many parts of the USA, rightfully so, given the fact that a good portion of the cell phones are sold inside a prison by those people within government organizations that can be compromised by financial means. Communications between correctional officers and public safety officers are not at risk by a properly filtered and engineered system.

2. Devices and Frequency Bands

The only technology that can prevent the use of any and all frequencies, protocols etc. is jamming.

Inmates currently use other technologies include walkie talkies, and Wi-Fi. However the materials used in these technologies are not as common as in cellular communication. A cell phone can be used anywhere anytime, without the need of special equipment or knowledge of its properties. That is why for the most part other technologies were never reached the threat level of cell phones.

It has been our experience that the goal for suppressing communication has been to balance the funding of such a system with the actual threat. For cell phones the threat is pandemic. Therefore blocking cellular communication would solve 90-95% of all illegal communications within a prison.

3. Interference to Other Radio Services

Jamming can be set up to insure that the signal levels that it produces are substantially less than those transmitted by the towers to the same area located outside the prison. The location of antennas, the power levels used, and the control of the type of jamming protocol (type of noise, packets etc.,) can be a determining factor. Each prison has different signal levels and propagation patterns from the surrounding cellular towers and therefore each prison must be designed, and commissioned separately.

The quality of the amplifiers used in the design of a jamming system as well as the type of filtering used will determine the unwanted products that interfere with out of band communication. They can be minimized and eliminated through proper engineering.

By using certain techniques our company has been able to refine jamming to be more dynamic in nature adjusting its power levels to those of incoming signals. However, we believe a static level is far superior to dynamic if there is a requirement to 100% jam any and all transmissions due to security levels of the prison.

Our experience indicates that the cellular providers can measure the influence of jamming on their network, and provide information that is essential for us to adjust the jamming propagation pattern to satisfy any and all concerns.

As well, we have simple monitoring techniques that we deploy to insure that jamming does not interfere with cell phone communication outside the perimeter of the prison. These techniques are 24/7monitored.

The biggest problem we have experienced is when the operator decides to increase their signal levels in attempt to counter the jamming signal inside the prison. This occurs in countries where the inmate can compromise an engineer or technician within the employ of the cellular carrier.

4. Protecting 911 Calls and Authorized Users

In our managed access system Cell Phone Controller that we offer, 911 calls are never affected since every cell phone that is denied service is still allowed to make a 911 call.

With regard to jamming, if the system is properly engineered, and the signal levels of the jamming units are much lower than any outside the prison and does not affect 911 calls by the public.

5. Cost Considerations

Jamming systems provide the best and most economical way of preventing the use of cell phone by inmates. Once installed, the only operating cost is the monitoring of the system and the SLA agreements. The capital cost of the system is dependent on the incoming tower signal levels, the nature of the threat, the areas needed to be covered, and the prison size.

Jamming systems require very little if any interaction with the staff. This is important since compromise of any system is inevitable given access to it.

For Cell Phone Control systems the costs associated are similar to that of jamming, whereby all that is needed is an ongoing maintenance agreement.

The comparison of the CPC versus the jamming system comes into play based on several factors. We believe that jamming offers the best value with prisons with less than 2000 inmates. For large prisons greater than 2000 inmates, or multiple campus configurations, CPC becomes more advisable and economical.

However, the need for multiple methods and strategies makes it imperative to deploy dynamic techniques in mitigating any cell phone risks. In many cases both CPC and jamming must be utilized and properly engineered.

Final Comment: CellAntenna offers alternate methods of procurement for our systems. One of the best methods is to engage our cell phone suppression services. We supply all of the equipment, and the engineers. We fully monitor the system 24/7 and utilize all legal means to eliminate the threat of cell phones in a prison. By using our service, the capital costs remain low, and the prison authorities have access to the latest methods and techniques as they become available. We currently offer the Cell Phone Control , and Reactive Suppression solutions as a service.

6. Locating Contraband Phones

The benefit of managed access and jamming is that there really is no need to locate where the cell phone is, only that it is disabled. This is an important concept; since most people involved in correctional institutions do not want spend their time looking for a cell phone. They want the problem to go away so that they can go back to the days where they were looking for important items like, guns knives and other contraband. In both the CPC system and jamming, spending public funds looking for phones is not required.

7. Regulatory/Legal Issues

The 1934 Communications act deals only with legal communication. The act specifically states that local and state governments cannot interfere with Licensed and Authorized communication. The fact is that the cell phone is illegal to use in a prison. It is therefore not licensed or authorized and can be stopped. The application of this law by the FCC has always been suspect as they do have the right under the 1934 Communication Act to clear this up.

As well it is equally irresponsible to allow any commercial enterprise to have control over any jamming or cell phone control system. It is important that security issues be handled by the department of corrections and that no Cell phone carrier can shut any system down by simply filing a complaint. This is what is proposed in many regulations where the carrier is concerned that the system deployed in a prison may affect their legitimate revenue. However, national security should always come before commercial enterprise. Should a carrier have a problem with a particular jamming system installed in a prison, they should provide evidence and allow the facility to adjust the power levels of the jammer to insure that there is no interference.

8. Technical Issues

The use of any technology to find cell phones is a waste of public money. Jamming and CPC technologies provide the correctional facility the ability to control the pest of cell phones and eliminate its security threat.