



America's Leader in Partnership Corrections

Harley G. Lappin
Executive Vice President
Chief Corrections Officer

January 3, 2012

Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Received & Inspected

JAN 17 2012

FCC Mail Room

Subject: FCC Petition For Rule Making Filed by CellAntenna Corp on September 2, 2011

To Whom It May Concern:

We have read this FCC Petition that was recently filed by CellAntenna and support this effort to defeat the use of contraband cell phones in correctional facilities. Having the carriers collaborate with corrections officials in the US, to develop and implement a mutually acceptable process for disconnecting contraband handsets detected in our facilities, would be a major step forward and would give our correctional administrators a very helpful tool for maintaining the security of their facilities.

Regards,


Harley G. Lappin

No. of Copies rec'd 0+3
LH ABCDE
WTB 12-1

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)
)
Amendment of Section 20.5 of the)
Commission's rules, 47 C.F.R. § 20.5) _____
To Categorically Exclude Service)
To Wireless Devices Located on)
Local, State, or Federal Correctional)
Facility Premises)

Petition for Rule Making

Received & Inspected

JAN 17 2012

FCC Mail Room

CELLANTENNA CORPORATION
12453 NW 44th Street
Coral Springs, Florida 33065

Marjorie K. Conner
700 West View Terrace
Alexandria, Virginia 22301
Its Counsel

September 2, 2011

Table of Contents

Summary	i
CellAntenna	1
The Problem	2
NTIA Notice of Inquiry	3
a. Jamming	3
b. Managed Access	5
c. Detection	6
Simple Solution	7
CMRS Provider Cooperation	8
Changes to the Commission's Rules	10

Summary

The possession and use of contraband wireless devices is increasingly a problem in correctional facilities. Regardless of the size, location, security level or design of the correctional facility, most have located and seized contraband wireless devices.

In its recent Notice of Inquiry, the National Telecommunications and Information Administration (“NTIA”) asked for comment on three different technological approaches to eradicating contraband wireless devices: jamming, managed access, and detection.

Through the comments before NTIA, it is clear that CMRS providers believe that jamming creates interference; and corrections officials believe managed access is too complicated and expensive. Carriers and corrections officials embrace detection as a means to eradicate contraband wireless devices in correctional facilities.

CellAntenna believes that detecting contraband wireless devices is just the first step. The Commission must modify its rules to require CMRS providers to suspend service to wireless devices reported to be operating illegally in correctional facilities, so that they may be disabled in a sure-fire and cost-effective manner.

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)
)
Amendment of Section 20.5 of the)
Commission's rules, 47 C.F.R. § 20.5) _____
To Categorically Exclude Service)
To Wireless Devices Located on)
Local, State, or Federal Correctional)
Facility Premises)

Received & Inspected
JAN 17 2012
FCC Mail Room

Petition for Rule Making

CellAntenna Corporation ("CellAntenna"), by counsel, and pursuant to Section 1.401 of the Commission's rules, 47 C.F.R. § 1.401, petitions the Commission to revise its rules to make clear that Commercial Mobile Radio Service providers, as defined by Section 20.9 of the Commission's rules, 47 C.F.R. § 20.9, must suspend service to contraband wireless devices reported to be operating inside correctional facilities.¹

1. CellAntenna

CellAntenna, Inc. ("CellAntenna") is a family-owned US company, based in Coral Springs, Florida. Since 2002, CellAntenna has led the industry in marketing and servicing communications devices. In the course of its business, CellAntenna has developed a special expertise in ferreting out contraband wireless devices within correctional facilities. CellAntenna has developed sophisticated equipment which can jam contraband wireless devices in correctional facilities with laser-like precision. CellAntenna also has developed a program by which contraband wireless devices can be detected and identified within correctional facilities by serial number, *i.e.*, ESN/MIN for

¹ "Correctional facility" means any place for the confinement or rehabilitation of offenders or individuals charged with or convicted of criminal offenses. 42 U.S.C. § 3791

CDMA units and IMEI/MSI for GSM/UMTS units. Importantly, CellAntenna's detection system also identifies the carrier providing service to the contraband wireless device.

2. The Problem

The possession and use of contraband wireless devices is increasingly a problem in correctional facilities. Regardless of the size, location, security level or design of the correctional facility, most have located and seized contraband wireless devices.

Contraband wireless devices have been used to aid an inmate's escape from a Kansas prison,² to threaten innocent civilians,³ to organize a strike among inmates at several Georgia prisons,⁴ to approve targets for robberies.⁵

Correctional officials note that so-called smart phones have ramped up the stakes by offering Internet access. With a smart phone, "a prisoner can call up phone directories, maps and photographs for criminal purposes ... Gang violence and drug trafficking ... are increasingly being orchestrated online, allowing inmates to keep up criminal behavior even as they serve time."⁶

According to the *New York Times*, wireless devices are prohibited in all state and federal prisons in the United States, often even for top corrections officials.⁷ The mere

² Burke, Tod W., Ph.D. and Stephen S. Owen, Ph. D. , "Cell Phones as Prison Contraband," *FBI Law Enforcement Bulletin*, citing Thompson, Don, "Prisons Press Fight Against Smuggled Cell Phones," *ABC News*, <http://abcnews.go.com/Technology/wireStory?id=7332293>

³ *Id.*, citing Graczyk, Michael, "Texas Prisons Locked Down After Death-Row Inmate Found with Phone", *CorrectionsOne*, <http://www.correctionsone.com/corrections/articles/1747630-Texas-prisons-locked-down-after-death-row-inmate-found-with-phone> (accessed August 30, 2011).

⁴ Severson, Kim and Robbie Brown, "Outlawed, Cellphones are Thriving in Prisons," *The New York Times*, January 2, 2011.

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

possession of a phone or a wireless device in a federal prison is a felony, punishable by up to a year of extra sentencing.⁸

Even so, the problem of contraband wireless devices persists. A recent editorial in the *Los Angeles Times* complained that “mass murderer and renowned psychopath Charles Manson was sending texts to folks outside prison walls using a flip phone that he kept hidden under his mattress.”⁹ In the first six months of 2011, the California Department of Corrections and Rehabilitation (“CDCR”) confiscated more than Seven Thousand Two Hundred (7,200) contraband wireless devices within its correctional facilities.¹⁰ There is reason to believe this is just the tip of the iceberg.

3. NTIA Notice of Inquiry

In May, 2010, the National Telecommunications and Information Administration (“NTIA”) issued a Notice of Inquiry (“NOI”) on the use of contraband Cell Phones in Prisons.¹¹ In its NOI, NTIA asked for comments on various technological approaches to help corrections officials block or reduce unauthorized use of wireless devices by inmates. NTIA particularly asked for comment on three categories of contraband wireless device intervention: jamming, managed network access, and detection.

A. Jamming

NTIA described jamming as “the deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of disrupting use of electronic devices, equipment, or systems.”¹² A jamming device transmits on the same radio frequencies as

⁸ Cell Phone Contraband Act, codified at 18 U.S.C. 1791(d)(1)(F).

⁹ “Cut Off Cellphones in Prison Cells,” *Los Angeles Times*, August 14, 2011.

¹⁰ Stanton, Sam, “California Prison Officials Shutting Down Inmates’ Facebook Pages,” *Sacramento Bee*, August 9, 2011.

¹¹ Preventing Contraband Cell Phone Use in Prisons, Docket No. 100504212-0212-01, 75 Fed. Reg. 26733 (May 12, 2010).

¹² 75 Fed. Reg. 26734.

the wireless device, disrupting the communication link between the phone and the wireless base station, essentially rendering the hand-held device unusable until the jamming stops. NTIA noted that jamming devices do not discriminate between contraband and legitimate wireless devices – all are disabled within the range of the jamming device. NTIA also noted that currently, operation of jamming devices violates Sections 301, 302a, and 333 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 301, 302a, and 333. Several petitions for relief from these restrictions have been filed with the FCC.

CellAntenna supports efforts to allow jamming wireless device signals in correctional facilities as a comprehensive solution which may be implemented by correctional facilities without the cooperation of the CMRS providers.

CMRS providers oppose the use of jamming technology. Although each of them expresses its opposition uniquely, generally, they claim that if jamming technology is authorized, wireless networks will fail to operate properly and calls – particularly public safety calls – will be completed because of interference from operation of jamming technology.

CellAntenna notes that the CMRS providers' fears are ill-founded. NTIA recently conducted a test of jamming equipment.¹³ CellAntenna is familiar with the test because it provided the equipment for the test. As the report demonstrates jamming equipment is effective. Further specific recommendations were made to support the future use of a jamming technology.

¹³ Sanders, Frank H. and Robert H. Johnk, "Emission Measurements of a Cellular and PCS Jammer at a Prison Facility,": NTIA Report TR-10-466, May, 2010, <http://www.its.bldrdoc.gov/pub/ntia-rpt/10-466/10-466.pdf> (accessed September 2, 2011).

CellAntenna argued its position more fully in its response to NTIA's NOI. Until the issues raised in the NOI are resolved and operation of jamming equipment is allowed, jamming remains a dream of an efficient means of controlling use of contraband wireless devices in correctional facilities.

B. Managed Access

NTIA also requested comment on the merits of managed access systems. Managed access systems intercept calls to allow corrections officials to prevent inmates' access to carrier networks. The signal is not blocked, but is captured (or re-routed) so that communication with the base station is effectively interrupted. Managed access allows completion of calls from legitimate wireless devices.

Managed access is accomplished through a variety of processes, but all deny service to wireless devices not known to be legitimate. Managed access is popular with CMRS providers because of its ability to discriminate against contraband wireless devices, while preserving service to legitimate devices. Wardens find managed access difficult because it requires costly negotiation of a capacity lease with each CMRS provider and because deployment is complicated and costly. Wardens also note that managed access is not completely effective. CellAntenna has demonstrated that some managed access systems can be easily defeated with common wireless devices readily available to prisoners.

In order to function properly – and capture all types of wireless devices – the managed access must include all frequencies and frequency ranges being accessed by the wireless devices, legitimate and contraband, within the facility. Each CMRS provider serving the geographic region in which the correctional facility is located must cooperate

by entering into a spectrum lease agreement with the correctional facility. Generally, throughout the United States, agreements with each of AT&T, Verizon, Sprint and T-Mobile (the “Big Four”) must be obtained. Locally, there may be other carriers with whom the correctional facility must reach agreement. The time and resources invested in the negotiation for the spectrum lease create an unacceptable burden for correctional facilities.

Additionally, as with all technology, the moment a managed access system is deployed, it may be rendered obsolete by new developments in the industry. Managed access equipment must be scalable and adaptive so that it may remain effective over time. Questions about the return on the investment in managed access equipment, spectrum leases with CMRS providers and training corrections personnel to operate the equipment make managed access another dream, unavailable to most correctional facilities.

C. Detection

NTIA described detection as the process of locating, tracking, and identifying various sources of radio transmissions. Detection triangulates a wireless device signal and requires the use of correctional staff to physically search a small area – a prison cell – to seize the identified contraband wireless device.

Of these three technological approaches to eliminating contraband wireless devices in correctional facilities, clearly detection is the least technologically invasive. In its comments in response to the NTIA NOI, T-Mobile noted that detection systems are preferable to jamming because they can allow prison officials to locate, monitor over time, and intervene with users of contraband cell phones, but they do not interfere with

crucial public safety or other legitimate communications.¹⁴ But the ensuing physical searches are time (and resource) consuming and can be dangerous for correctional personnel. A better use of detection equipment can be made with the CMRS providers' cooperation.

4. Simple Solution

NTIA's NOI clearly identified detection as a robust tool currently used in eradicating contraband wireless devices in correctional facilities of all sizes.¹⁵ CTIA agrees, "[c]ell detection technology helps meet the [objective or eradicating contraband wireless devices] while preserving authorized communications in and surrounding correctional facilities."¹⁶

CMRS providers agree that detection is a preferred means of eradicating contraband wireless devices in correctional facilities, but it is only part of the solution. CellAntenna's equipment is capable of identifying – with specificity – wireless devices operating within correctional facilities. CellAntenna can provide a Warden device-specific serial numbers (ESN/MIN or IMEI/MSI) and can identify the service provider for the device.

As NTIA's NOI observed, when CellAntenna's equipment identifies a contraband wireless device, the Warden must deploy a team of correctional officers to search the facility to find and destroy the device. The physical search is time consuming and is not always successful. In contrast, if CMRS providers were required to suspend service to contraband wireless devices, the threat of harmful use of any device would be eradicated

¹⁴ Comments of T-Mobile USA, Inc., NTIA Docket 10054212-0212-01, Filed June 11, 2010, at 9.

¹⁵ Many detection devices are reasonably portable. They may be moved about in larger institutions to realize greater benefit for the cost of equipment.

¹⁶ Comments of CTIA – The Wireless Association®, NTIA Docket 10054212-0212-01, Filed June 11, 2010, at 17.

in a fraction of the time – and at a fraction of the cost – consumed by a physical search and destroy mission.

CellAntenna proposes a three step plan:

1. The correctional facility performs a sweep electronically by using equipment that identifies certain unique characteristics of a wireless device through radio frequencies.

2. By electronic mail or facsimile, the Warden transmits to the CMRS provider identifying the contraband wireless device by ESN/MIN or IMEI/MSI (“Notice of Contraband Wireless Device”).

3. The CMRS provider must 1) send a warning to the identified contraband device by Short Message Service or “SMS” that the device is operating illegally; and 2) suspend service to the contraband wireless device within one hour after receipt of the Notice of Contraband Wireless Device.

5. CMRS Provider Cooperation

The three step plan only works when the CMRS provider follows through to suspend service to the contraband wireless device.

Recently, Facebook reached agreement with the California Department of Corrections and Rehabilitation to shut down inmate pages that have been set up by prisoners using contraband cellphones.¹⁷ The Facebook agreement came after Reuters reported that a child molester in a California prison used Facebook to gather current information about one of his victims from behind bars and then mailed her family some

¹⁷ Evangelista, Benny, “California Cracks Down on Prisoner Facebook Accounts,” *San Francisco Chronicle* (online *SFGate.com*), August 9, 2011, http://www.sfgate.com/cgi-bin/blogs/techchron/detail?entry_id=95027 (accessed September 2, 2011).

drawings of the girl, showing her current hair style and brand of clothing, ten years after his original crime. Facebook spokesman, Andrew Noyes said:

We will disable accounts reported to us that are violating relevant U.S. laws or regulations or inmate accounts that are updated by someone on the outside.¹⁸

Facebook's agreement is a gracious step toward eliminating the evils that flow from prisoner use of wireless devices, including access to social media. Even so, as Facebook's Mr. Noyes noted, because wireless devices are prohibited in all correctional facilities, in most instances, prisoners should never have access to the communications conduit that puts them in touch with Facebook.¹⁹

Facebook has agreed to shut down inmate pages, citing its user agreement that prohibits illegal activity on Facebook. Each of the CMRS providers includes a similar clause in its customer agreements.²⁰ Despite an absolute right to shut down prisoner use of contraband wireless devices, no carrier has stepped up in the way that Facebook has.²¹

This is true even though the Title 18 has been amended to criminalize possession of a wireless device in a federal correctional facility and that most states have similar laws. The Commission must order CMRS providers to do the right thing and shut down contraband wireless devices once CMRS providers are aware that they are operating from correctional facilities.

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ See e.g., "My Verizon Wireless Customer Agreement," <http://www.verizonwireless.com/customer-agreement.shtml> (accessed September 2, 2011), Under What Are Verizon Wireless' Rights to Limit or End Service or End this Agreement?; AT&T Wireless Customer Agreement, which incorporates its Acceptable Use Policy, <http://www.corp.att.com/aup/> (accessed September 2, 2011).

²¹ With respect to contraband wireless devices in federal prisons, the CMRS providers who refuse to suspend service to the contraband devices run the risk of prosecution for aiding and abetting continuing violations of Section 1791(d)(1)(F) of the Criminal Code, 18 U.S.C. § 1791(d)(1)(F).

6. Changes to the Commission's Rules

To this end, CellAntenna proposes that the Commission add to Section 20.15(a), 47 C.F.R. § 20.15(a), new subsections (1) and (2) as follows:

(1) If a CMRS carrier receives notice from a Warden or other ranking official at a correctional facility that a wireless device served by that CMRS carrier is operating within the confines of the correctional facility, it shall suspend service to the identified wireless device within one (1) hour after receipt of the notice.

(A) The notice from the Warden shall be in writing and may be transmitted by facsimile or by means of electronic mail.

(B) The notice from the Warden shall include the ESN/MIN or IMEI/IMSI, as the case may be, for the wireless device, as well as any other identifying information available to the Warden.

(2) No CMRS provider suspending service under subsection (1) above will be held to have violated any law, rule or regulation of the FCC:

(A) so long as its action to suspend the service was taken in good faith reliance on a Warden's notice; and

(B) if presented with compelling evidence contradicting the Warden's notice, the Carrier took immediate action to reinstate the suspended service.

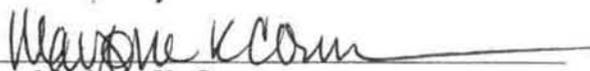
CellAntenna's proposed rule puts the responsibility for management of contraband wireless devices precisely where it belongs: in the hands of CMRS providers.

CellAntenna is uniquely situated to see the full array of options to combat the use of contraband wireless devices in correctional facilities. While jamming is the most efficient means of ending the abuse, CellAntenna acknowledges the controversy surrounding deployment of jamming devices. In the face of that opposition, and the general agreement that detection is an acceptable, non-invasive means of combating wireless devices, CellAntenna recommends that the Commission take advantage of

existing technology and require CMRS providers to do their part and suspend service to any wireless device reported to be operating in a correctional facility within one hour after receipt of notice from a Warden.

Respectfully submitted,

CELLANTENNA CORPORATION

By: 
Marjorie K. Conner
Its Counsel

700 West View Terrace
Alexandria, Virginia 22301
(703) 706-5917
mkconner@mkconnerlaw.com
September 2, 2011

For Immediate Release

Media Contact: Ms. Priscilla Doyle
Ph: (954) 340 7053 Ext 2203
pdoyle@cellantenna.com

JAN 17 2012

FCC Mail Room

CellAntenna Files Petition with the FCC to have Illegal Cell Phones Found in Prisons Turned Off by Cell Phone Carriers

Cooperation between Cell Phone Carriers and Law Enforcement: Essential to Solve the Problem of Contraband Cell Phones Use In Correctional Facilities.

Coral Springs, FL/September 6, 2011 - CellAntenna Corporation announced that they have filed a petition to have illegal cell phones in a prison that are electronically detected and identified, unsubscribed by the cellular carriers. The petition requests that the FCC define rules for how law enforcement and cellular carriers can help curtail the illegal use of cell phones in prisons by criminals.

Illegal cell phones in prisons are a security threat to law enforcement and the general public. This position will no doubt be confirmed by a report due out this week by the Government Accountability Office (GAO). All too often the inmate obtains a smuggled cell phone and uses it to continue their crime behind bars. No matter how vigilant correctional officers are the infiltration of cell phones has escalated to pandemic proportions - with hundreds of thousands of cell phones found annually in our nation's prisons. Although jamming technology would be the most cost effective way to solve the problem, current laws prevent its deployment. Other methods including managed access do not solve the problem and can be easily defeated and is too expensive for local and state departments of corrections.

CellAntenna has perfected an affordable and practical technology to stem the problem. CellAntenna's *Guardian Service* detects and identifies individual cell phones and the subscribing carriers. This method identifies cell phones in a targeted area by the carrier and creates a simple list that can be sent to the carriers by the corrections authorities indicating the cell phones that are being used illegally in the prison. The carrier has only to unsubscribe the cell phone from their system rendering the illegal device useless (passive service denial). By repeating the process, like a 'pest control' service, the cell phones would be turned off and the problem solved with minimal cost. The petition filed recognizes that the carrier cooperation is essential to effectively fight the problem of illegal cell phones possession and use in prisons.

"In our discussions cellular service providers expressed their desire to help solve the problem of illegal cell phones in the prisons" stated Howard Melamed CEO of CellAntenna Corp. "Having the FCC provide the framework, by way of our petition assists the carriers and law enforcement officers in protecting the public by thwarting the illegal use of cell phones by criminals."

CellAntenna in cooperation with Department of Corrections around the country has tested the Guardian Service solution and can attest to the amount of illegal cell phones found in prisons and their specific details.

For more information please contact Bruce Buckley at bbuckley@cawireless.com or at 860-391-3364.

About CellAntenna: CellAntenna is an experienced system integrator that specializes in cell phone control solutions. . CellAntenna's Detection, Managed Access, Guardian Service and Cell Phone Jamming solutions are used by governments around the world as well as the US Federal Government. For nearly a decade, the company has increased its clients' productivity and safety through the boosting of signal strength and reduction of dropped calls using cellular repeaters and mobile phone signal boosters. Headquartered in Coral Springs, FL, CellAntenna, a woman owned ISO 9001 2008 company also has offices in Europe.. More information is available at www.cellantenna.com , www.cjam.com and www.cawireless.com.

####



WHITE PAPER

Contraband Cell Phone Defeat Cell Antenna's Solutions Portfolio

Guardian Service

Prepared By:
CellAntenna Corp
12435 NW 44th St
Coral Springs, FL 33065
954-340-7053
www.cawireless.com



1.0 Introduction

The possession and use of contraband cell phones in correctional facilities is a global problem and the USA is no exception. There are a number of well documented and publicized crimes that have been orchestrated by inmates using contraband cell phones as a means to communicate with accomplices on the outside. These crimes include but are not limited to murder, attempted murder and witness intimidation.

Every correctional facility is different:

- Location (rural/urban)
- Offender population (300 – 5,000)
- Security level (maximum/medium/minimum)
- Circa (early 1800's to present day)
- Size (square feet to acres)
- Design (distributed 2 story PODs – large multi-floor cell blocks)

This diversity means that the solutions to defeat the possession and use of contraband cell phones in this myriad of correctional facilities must be diverse as well. For this reason, CellAntenna over the past three (3) years has invested in R&D to develop a portfolio of solutions.

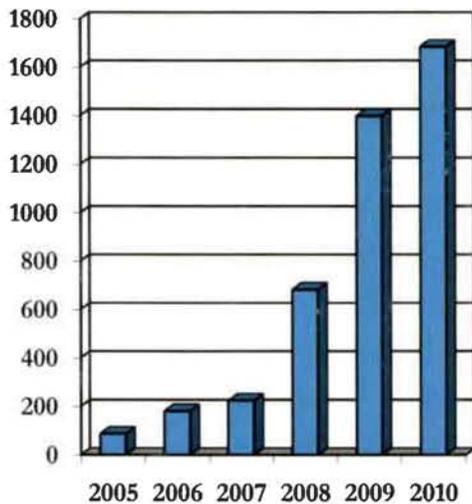
- Simple detection
- Intelligent detection and control
- Service denial (outside of USA)
 - Jamming
 - Handset suppression
 - Protocol disruption
- Managed access

This White Paper is intended to provide an overview of cell phone threat management alternatives for correctional facilities with a focus on the benefits of one solution. This solution, the Guardian Service is a service based alternative which relies on collaboration between the cellular carriers and the state/federal corrections officials. This collaboration includes the disconnect of cellular service (passive service denial) of contraband cell phones (plus SIM cards) detected and identified in a specific correctional facility. This detection, identification and verification is accomplished using state of the art non intrusive technology that was originally developed for the US military and is in use today in combat theatres (non-classified).

2.0 History

Corrections departments at all levels (county, state & federal) have invested time and money to improve security in an attempt to thwart the smuggling of cellular handsets and SIM cards into correctional facilities. Consequently, residential housing unit and personal searches have become more frequent (labor intensive for the corrections officers and confrontational). In addition, specially trained dogs have been used that sniff out the lithium batteries used in most cell phones. The harsh reality is that all of these initiatives have not reduced the number of handsets in use today by offenders. Quite the contrary as these graphics on the next page will show:

Tennessee DOC – Confiscated Cell Phones



In California in 2009 the number of confiscated cell phones in state correctional facilities alone exceeded 7,000



"Jamming" is one of many techniques for defeating the use of a cellular telephone and any correctional professionals view jamming of cell phones, in use inside of correctional facilities, as the best technology solution because of its' simplicity.. In the US, UK, Canada and Australia jamming is illegal .for all except the military (national security). The main problem with jamming is that the propagation of RF signals can be unpredictable and as such effect the cellular service outside of the intended target area in the surrounding community. Legislation that would enable the FCC to grant waivers to the jamming law (Communications Act of 1934) was passed in the US Senate in 2009 and was never brought to the floor of the House of Representatives for a vote in 2010.

With jamming eliminated as an alternative for the foreseeable future, state, local and federal correctional professionals in conjunction with industry associations began to evaluate the various technologies that were available. For example:

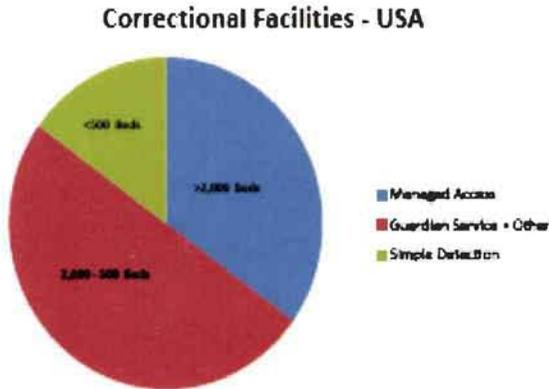
- Localization (similar to GPS but triangulates using three system antennas)
- Simple detection (handheld devices that alert on a call attempt)
- Intelligent detection (detects and indentifies handsets by their unique serial number)
- Managed Access (attracts contraband handsets onto the system-essentially blocking calls)

What is interesting is that all of these solutions are viable in the right environment. As stated earlier, every correctional facility is different and as such one single solution cannot be effective in terms of ubiquitous cell phone defeat or cost. This reality was substantiated during a National Institute of Justice (NIJ) Workshop in early 2011 by Jon Ozmint (Commissioner – Corrections South Carolina) when he stated "what is needed is a tool box of alternatives". CellAntenna recognized this fact almost 3 years ago and began developing a portfolio of solutions in 2008. All other companies competing in this industry offer single point solutions which limit their ability to serve the diverse requirements of many corrections organizations around the world.

- Tecore – Managed Access
- DRT (Shawntech) - -Managed Access
- ITT – Localization
- Berkeley Vetronics – Simple Detection

3.0 The Issue

Today Managed Access is the solution that the CTIA and many correctional professional believe "is the answer" and a practical alternative to jamming. This is a well founded conclusion which CellAntenna supports, if the requirement is for correctional facilities in excess of 2,000 beds. For unlike other cell phone threat management solutions, a Managed Access system does not scale (downward) in terms of cost and consequently becomes less cost effective for smaller (less than 2,000 beds) facilities.



With this in mind, if you consider that correctional facilities in excess of 2,000 beds comprise approximately 35% of the total of county, state and federal correctional facilities, then approximately 65% of correctional facilities in the USA are in need of an alternative that is effective and affordable.

CellAntenna believes that the Guardian Service can be an effective and affordable solution for a large percentage of these less than 2,000 bed correctional facilities.

The Guardian Service is not a competing technology for Managed Access. Quite the contrary. It is complimentary and is simply another solution in the "tool box" that will help corrections officials defeat the use of contraband handsets and in some instances save lives

4.0 Guardian Service

CellAntenna has launched the Guardian Service after one year of engineering and field testing (Reeves County – Federal Prison Pecos, TX). The Cell Phone Control (CPC) unit is essentially the same platform that is used to deliver CellAntenna's Managed Access solution.



Portable Unit



The Guardian Service uses a CPC portable form factor

For Managed Access a rack mountable 19" chassis – 5U CPC is used.

Rack Mount Unit



- In Guardian Service mode the CPC detects and controls contraband handsets and does not manage the access of cell phones in the target area
- The system ultimately defeats the use of contraband cell phones by detecting the handset and discovering the unique serial number of the handset (IMEI/IMSI – GSM/UMTS & ESN – CDMA),
- ***An important part of the process is verifying the list of discovered handsets as being in used inside of the correctional facility and then submitting a vetted list to the subscribing carrier for disconnect (passive service denial)***
- Passive service denial can be applied to GSM, CDMA and UMTS handsets (Managed Access does not currently support UMTS due to the improved security features of the UMTS protocol.)
- Similar to Managed Access the Guardian Service uses a distributed antenna system (DAS) to predictably propagate the system signals.
- However there are differences in DAS design as the desired end result is different. Studies have shown that 75% of all contraband cell phone use in correctional facilities originates from the inmate housing units in the evening (19:00-01:00). Consequently, the DAS is installed only in the housing units. ***This reduces the cost of the Guardian Service DAS by as much as 60% relative to the DAS required to support a Managed Access system***
- Another benefit of installing the DAS inside of the housing units is that controlling system signals (CPC) is more predicable than a ubiquitous DAS needed for a Managed Access system.
 - The transmit power levels of the DAS antennas can be lower as the carrier's cellular signals are naturally attenuated inside a housing unit complex by as much as 10-15 dBm. Result: Low power = reduced emissions outside of the buildings.
 - In addition to lower power being needed for the DAS antennas inside the housing the system signals (Guardian Service) are naturally attenuated by the housing unit building (typically steel re-enforce concrete). Again, by as much as 10-15 dBm. Consequently, an already low power signal is further attenuated by the building structure. Result: Probability of the system signals (Guardian Service) radiating beyond the designated target area is substantially reduced relating to a ubiquitous DAS needed for a Managed Access system.
- The Guardian Service DAS is permanently installed in the correctional facilities' housing units.
- ***However, the detection, identification of handsets and the verification of the list of discovered handsets, based on the size of the facility, can be 3-5 day event. . This means the Guardian Service Cell Phone Controller (CPC) can be shared by 5-6 correctional facilities.***
- CellAntenna's experience is that approximately 80% of the contraband handsets will be detected and defeated over time.

During the aforementioned NIJ Workshop one of the themes reiterated by all participants called for "effective and affordable" solutions (plural). If the Guardian Service can defeat 80% of the contraband handsets in use in a correctional facility using passive service denial (collaboration with the cellular carriers) and do so at approximately 65% less than a Managed Access system, most would agree that this is a good deal.

5.0 Passive Service Denial

A key element of the Guardian Service is the cooperation and collaboration of the cellular carriers. Like all new concepts there are legitimate concerns. Some are legal, others are technical and some are process related.

1. In majority of the states in the USA, laws have been passed by the state legislature making it illegal to possess and use a cell phone inside of a correctional facility. The harshest penalty for use and possession is in the State of New Jersey where the maximum is 15 years.
2. President Obama in August of 2010 signed into law the Contraband Act of 2010 which classified cell phones as "contraband" inside of a Federal correctional facility and as such illegal to use and possess.
3. It is anticipate that for sites that will use the Guardian Service to defeat cell phone use a spectrum leases will be secured from the carriers by the State Department of Corrections.
4. This spectrum lease process will provide:
 - o A documented process to alert each carrier of a Guardian Service project
 - o An opportunity for the carriers to participate in the system testing before commissioning to ensure that system coverage is as designed.
 - o For an ongoing process for the cellular carriers and the State DOC to conduct regular audits to ensure continued compliance as the cellular carrier's macro network evolves i.e. system signals are not radiating beyond the designated target areas.
 - o An opportunity for all to design and refine a mutually acceptable process for list submission and service disconnect (passive service denial).

6.0 Conclusion

Correctional professionals around the world agree that based on the diversity of correctional facilities in each of their jurisdictions, in terms of size, design, location, etc., that the concept of the "tool box" of alternative solutions is a key element in the battle to defeat the use of contraband cell phones..

An example of the differences in correctional facilities in a state's jurisdiction is the State of Maryland where the population of their 23 facilities is from 150 – 2600 offenders.

Facility	Population
20. Poplar Hill Pre-Release Unit	150
18. Eastern Pre-Release Unit	174
21. Southern Maryland Pre-Release Unit	177
18. Baltimore Pre-Release Unit	189
15. Baltimore City Correctional Center	501
17. Central Maryland Correctional Facility	509
14. Eastern Correctional Institution Annex	585
19. Jessup Pre-Release Unit	589
3. Brockbridge Correctional Facility	641
2. Maryland Reception	661
22. Baltimore Central Booking and Intake Center	800
6. Maryland Correctional Institution for Women	842

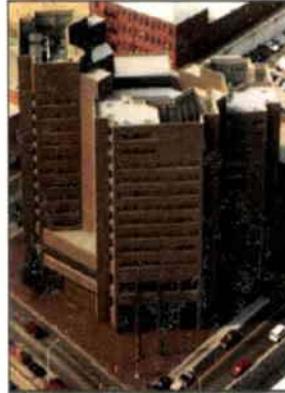
Facility	Population
12. North Branch Correctional Institution	868
7. Patuxent Institution	987
4. Jessup Correctional Institution	1024
1. Metropolitan Transition Center	1647
11. Western Correctional Institution	1687
5. Maryland Correctional Institution - Jessup	1722
10. Roxbury Correctional Institution	1744
8. Maryland Correctional Institution - Hagerstown	2035
9. Maryland Correctional Training Center	2483
13. Eastern Correctional Institution	2682
23. Baltimore City Detention Center	306

Another difference is the location in terms of rural or urban

Maryland Reception, Diagnostic and Classification Center
550 E. Madison Street
Baltimore, Maryland 21202
410-878-3500

Opened: 1967; relocated to present site in 1981
Number of Positions: 519
Total Operating Costs: \$39,585,631

Security: Administrative ~ All Levels
Adult Males
Average Daily Population: 661



Maryland Correctional Institution ~ Jessup
P. O. Box 549
Jessup, Maryland 20794
410-799-7610

Opened: 1981
Number of Positions: 371
Total Operating Costs: \$38,145,994

Security: Administrative ~ All Levels
Adult Males
Average Daily Population: 1,024



We applaud the CTIA for their support of Managed Access as a solution. However, the job is not done! Other solutions must be accepted and available to correctional officials so they can effectively and affordably solve the problem in all of their facilities (small/medium and large).

The Guardian Service is an alternative solution that has been proof of concept tested in more than 6 states in the USA and recently in England by the UK Foreign & Commonwealth Office (FCO - in support of the Ministry of Justice). The overwhelming consensus from all of these tests is that the Guardian Service is a much needed solution