

**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

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)

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