

**Before the Federal Communications
Commission Washington, D.C. 20554**

In the Matter of

Promoting Technological Solutions to
Combat Contraband Wireless Device Use in
Correctional Facilities

GN Docket No. 13-111

Cell Antenna Corp. Request for Amendment
of Section 2.807 of the Commission's Rules
(47 C.F.R § 2.807) to Allow the Use of
Radio Frequency Jamming Equipment by
Local and State Law Enforcement Agencies
and Emergency Response Providers

RM-11430

Petition of the GEO Group, Inc. for
Forbearance From Application of Sections
302,303, 333 of The Communications Act of
1934, as amended, And Sections 2.803 and
2.807 of the Commission's Rules to Allow
State and Local Correctional Authorities to
Prevent Use of Commercial Mobile Radio
Services at Correctional Facilities

ET Docket No. 08-73

CTIA — The Wireless Association Petition
for Declaratory Ruling Regarding the
Unlawful Sale And Use of Cellular Jammers
and Wireless Boosters and Repeaters

WT Docket No. 10-4

South Carolina Department of Corrections
Request for Authorization of Managed
Access Systems within Correctional
Institutions in Order to Improve Public
Safety Under Conditions that Protect
Legitimate CMRS Users

PRM09WT

Mississippi Department of Corrections
Request for Authorization of Managed
Access Systems within Correctional
Institutions in Order to Improve Public
Safety Under Conditions that Protect
Legitimate CMRS Users

PRM09WT

Global Tel*Link Corp. Request Amendment of Sections 22.3(b), 1.931 and Subpart X of the Commission's Rules and Creation of New Rule(s) To Authorize a Plurality of Technical Solutions to Eradicate the Unauthorized Use of Wireless Devices in Correctional Facilities

PRM11WT

CellAntenna Corp. Request for 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

PRM11W

COMMENTS OF SECURUS TECHNOLOGIES, INC

Securus Technologies, Inc. (“Securus” or “Company”), hereby respectfully submits its initial comments for the Federal Communications Commission’s (“FCC’s”) Notice of Proposed Rulemaking (NPRM) in the above referenced Dockets.

Introduction

Securus is authorized to provide Inmate Telephone Service (ITS) in all 50 states and the District of Columbia (DC). Securus currently serves approximately 2200 correctional facility sites (locations) in 46 states and DC. Securus provides its inmate service to State, County, and Local correctional facilities throughout its service territory. All inmate calls placed from facilities served by Securus require the called party to “positively accept” (authorize) the call by pressing a particular digit on the keypad before the call is connected. Additionally, on every Securus served facility collect call, the called party is given the option of hearing a rate quote, is

told how to reject the call before charges apply, and is given an option to block future calls from inmates at Securus served facilities. The Securus inmate telephone systems verify and validate inmate dialed numbers to assure they are allowed and to block calls to unauthorized numbers. Unauthorized numbers will include judges, law enforcement officers, victims, and witnesses to prevent inmates from intimidating or attempting to influence these individuals. Also, blocked numbers may include gang members or known criminal associates to prevent criminal activity from being conducted from behind the prison walls. All inmate calls, except to attorneys, are subject to monitoring and recording and could have voice verifications and “word spotting” to detect unauthorized activity both inside and outside the jail. These features, and others, allow Securus to provide a safe and secure telecommunication system in correctional facilities.

The use of contraband wireless devices allows the inmate to bypass the authorized telephone system and to circumvent all the safety and security features listed above. Contraband wireless devices create a serious security threat to the correctional institution staff, law enforcement officers, witnesses, judges and the public. Use of these contraband devices is a growing problem in correctional facilities and efforts to stop such devices from entering the jails and prisons are mostly unsuccessful. A much more effective solution is to render such devices useless within the confines of the correctional institution. If the devices do not operate within the jail or prison, there is no incentive to smuggle in such devices.

Detection and Suspension of Service to Contraband Wireless Devices

Efforts to stop the use of contraband wireless devices have concentrated on three possible types of systems – detection, managed access, and jamming. Each of these solutions has

advantages, disadvantages, varying costs and varying effectiveness. Below Securus will provide its understanding and perspective of each of these system types.

Detection - It is Securus' understanding that these systems are capable of detecting a cell phone or wireless device signal when the device is being used. If the wireless device is turned off, detection by the system is not possible. Therefore, detection occurs when a call is in progress and the detection system is not capable of ending the unauthorized connection. Some, if not all, of these detection systems are capable of giving a general location of the device within the facility and are capable of identifying the ESN/MIN or IMEI/MSI of the device which will identify the service provider. With a detection system, separate action is needed by the correctional facility and/or CMRS provider in order to prevent the continued use of the contraband wireless device. The correctional facility would need to search, find, and confiscate the detected device. Such action raises safety and security concerns for the corrections officers that must conduct such a search. Also, many inmates are skillful at hiding contraband devices or passing them to other inmates so the device is no longer located in the area the system detected. The CMRS provider of the detected device would need to terminate service to prevent future use. It is Securus' understanding that CMRS providers are reluctant to terminate service. All of the above actions take time and resources, during which time the contraband device is still capable of being illegally used by inmates. Although the detection system itself may be less expensive than some of the other systems, Securus believes without a commitment by CMRS providers to quickly terminate service, a detection system is the least effective system to eliminate contraband wireless devices, and it has other negative aspects, including correctional officer involvement and safety. Detection system effectiveness could be dramatically improved if CMRS providers

had a mandate to terminate service to the detected device within a very short time after notification by the facility or the provider delivering the detection system to the facility.

A relatively new form of wireless device detection is a highly portable body scanning device specifically designed to detect the components of cell phones, even when turned off. Cell phones are being manufactured with fewer and fewer metal components. Therefore, these specialized detection scanners are much more effective in finding contraband wireless devices than standard metal detectors. Additionally, because these scanners / detectors are very portable, they can be easily moved within the prison so inmates do not know when or where they may be subjected to a scan. The price of the scanning equipment is inexpensive as compared to other systems but correctional facility personnel costs must also be considered. As with other detection systems, the scanner requires additional action by corrections officials, such as; setting up the scanner, controlling inmates as they are scanned, and retrieving any contraband device that may be detected. These scanning devices are not capable of identifying signals to determine the CMRS provider nor are they capable of suspending the use of a cell phone that may elude the prison's scanning program.

Managed Access Systems – Managed access systems also detect signals only when the device is in use but these systems block the signal from being sent unless the detected device is on an authorized or approved list. The theory with this type of system is that it will not block the authorized cell phone signals of correctional officers, jail administrators, the general public that may be in close proximity to the jail, or calls to 911. However, this requires that all the “authorized” device identifications must be contained in the managed access system database. This also requires that all calls to 911, from an authorized or unauthorized device, not be blocked. Inmates are prohibited from dialing 911 from the approved inmate telephone system to

prevent inmates from flooding the 911 system with false claims of emergencies. It is Securus' understanding that false calls to 911 by inmates with contraband cell phones were a major concern when managed access systems were tested. This has resulted in managed access systems being programmed to also block 911 calls from non-authorized devices. Thus, only authorized devices will be permitted to complete calls of all types. The administration of such a system is time and resource intensive – who manages the authorized device list, what is the criteria for a device to be placed on the list, who has the authority to add or remove a device from the list, and how do you prevent an inmate from receiving a device that is on the authorized list. Securus has learned that the overwhelming majority of contraband wireless devices are smuggled into the facilities by employees of the corrections institutions. Therefore, if these same employees have “authorized” cell phones that are then smuggled to inmates, the system would not only fail to detect the inmate's illegal use of the contraband device but would actually authorize such use. A managed access system would be more effective than a detection system but the equipment and resources to continually administrate the system make it the most expensive to operate.

Jamming – Jamming would block all wireless device signals within the jail or prison in which the system was installed. Critics of signal jamming express concerns that “bleed over” could jam the signal of a non-incarcerated person in close proximity of the jail or interfere with the radio communication systems of correctional officers. In some jail locations, the bleed over and proximity concerns may be justified but that is not true at many jail and prison locations. In Securus' experience, the majority of correctional facilities it serves do not allow anyone to have a cell phone or wireless device within the facility. This includes visitors and correctional facility employees. Therefore, any wireless device within the prison or jail would be considered a

contraband device. Additionally, many correctional institutions are in remote locations or, if located within a community, are positioned to not allow the general public in close proximity of the facility. The argument that cell phone jamming will interfere with the correctional facility's internal communication system can be easily dispelled by looking at the use of signal jamming technology by federal agencies today. One need only look at presidential events where, for security reasons, cell signals are jammed, yet the Secret Service communication system is unaffected. There is no question that signal jamming is the most effective way to stop the use of contraband wireless devices in jails and prisons. There is no external intervention needed to stop the unauthorized communication which is required with the detection systems. There is no way to game the system and have a contraband device placed on the "authorized" list or a requirement to constantly administer an authorization list which are the negatives of a managed access system. Jamming is also one of the, if not the, least expensive solutions to stopping the use of contraband cell phones in prison and jail facilities.

Which Detection and/or Suspension System should the FCC Endorse?

As clearly outlined above, each of the detection and/or suspension systems discussed has advantages and disadvantages. The FCC should not preclude any of these alternatives and should support the testing and implementation of all these options.

Which system would best serve a particular correctional institution should be determined by the facility location and the specific needs, including budgetary needs, and policies of the correctional institution. If a correctional institution is located in a highly populated area, or in some cases within a government building used for multiple purposes, signal jamming may not be appropriate and even managed access may not work due the administrative burden to keep an

accurate authorization list. If an institution has a policy of allowing correctional officers or employees to use wireless devices within the facility, signal jamming would not be a viable option. But, a facility that has a policy of banning the use of all wireless devices within the facility, including use by facility employees, and the facility is located so the public does not access the immediate area around the facility, then signal jamming should be allowed.

Who Pays for the Detection and/or Suspension System?

Considerable information has been provided regarding these various systems including system technical operations, system limitations, system administrative requirements, and the differing opinions about policies regarding the use of each type of system. However, Securus has seen very little about how the cost of these systems, regardless of which system is used, is to be recovered. The manufacturers and providers of the equipment, the system installers, the software providers, and the individuals that provide ongoing maintenance for these systems will all expect payment for their services. Most State, County, and Local government agencies are struggling to fund their limited budgets and many correctional authorities contend they are severely underfunded. So, who is going to pick-up the tab?

As an ITS provider, Securus is seeing an increasing number of Requests for Proposals (RFP's) that require a cell phone detection / suspension system be included in the bid proposal for the inmate phone system. Virtually every inmate phone service RFP requires that all services be provided at "no cost" to the correctional facility or government agency. Therefore, the ITS providers must recover these costs from the rates and charges generated from inmate calls completed over the authorized inmate telephone system. At a time when the FCC is questioning

the increasing costs ITS providers face and the rates they charge for calls placed by inmates, the provision of cell phone detection and suspension systems is an excellent example of how correctional institutions want and need the most advanced tools and latest technology to effectively operate their facilities but require the cost of these advancements to be recovered through inmate phone rates. Without exception regulators, legislators, inmate advocacy groups, correctional facilities and others consistently stress that prison safety and security are of paramount concern. The use of contraband wireless device detection and suspension systems are another step to enhance correctional facility safety and security. However, as with all such technological advances, there is a financial cost that must be recovered and the FCC should recognize these financial affects and consider them as they endorse or reject any of the possible options.

Conclusion

Securus believes all forms of contraband wireless device detection and suspension systems should be permitted. At a minimum, the three system types outlined above should be thoroughly tested. It is only through extensive testing that the FCC can place reasonable requirements on where or how a particular system type should operate. The FCC should take a firm stance that CMRS providers must cooperate with correctional facilities to quickly terminate service to detected contraband devices. The FCC should also strongly consider the needs and comments of the correctional institution industry. These are the people that often risk their lives or physical injury to enforce rules and policies to maintain safety and security. They should be afforded every possible option to assist in carrying out this difficult task. Finally, the FCC needs

to recognize each of these detection and suspension options has a financial cost that must be recovered.

Respectfully submitted,

Securus Technologies, Inc.

By: _____

Curtis L. Hopfinger

Director-Regulatory and Government Affairs

Securus Technologies, Inc.

14651 Dallas Pkwy, 6th Floor

Dallas, TX 75254

(972) 277-0319

July 18, 2013