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

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| | ) | |
| Wireless Service Interruptions | ) | GN Docket No. 12-52 |

To the Chiefs, Public Safety and Homeland Security
and Wireless Telecommunications Bureaus

# COMMENTS OF TECORE NETWORKS


**TECORE NETWORKS**

By: Stephen D. Hayes
Vice President and General Counsel

7061 Columbia Gateway Drive
Columbia, Maryland 21046
(410) 872-6000


April 30, 2012

## TABLE OF CONTENTS

**INTRODUCTION** ……... **1**

**COMMENTS**

**1. PAST PRACTICES AND PRECEDENTS**

**a. Under what circumstances have public agencies in the United States considered or effectuated interruptions of wireless service for public safety reasons?**..... **5**

*Contraband Wireless Devices and the Criminal Activity They Are Used to Conduct Warrant the Selective Interruption of Wireless Services in Corrections Facilities*

**b. What are relevant examples of foreign governments considering or effectuating interruptions of wireless service for public safety reasons? What laws or policies do foreign states have regarding interruption of wireless service for purposes of protecting public safety?**..... **11**

*Foreign Governments Have Permitted Wireless Interruptions Not Only for Public Safety but to Achieve a Variety of Other Goals*

**c. What are examples of wireless networks actually being used to put the public's safety at risk? Could interruption of wireless service have mitigated these harms? How would such interruptions have mitigated these harms?**..... **15**

*Inmates Have Increasingly Leveraged the Availability of Wireless Services to Obtain Cell Phones and Use Them to Engage in Dangerous Criminal Activity.*

*Managed Access Has Successfully Defeated Contraband Wireless Devices and Mitigated the Public Safety Risk*

**d. What existing policies do public agencies in the United States have for determining whether a service interruption is proper? What existing policies or agreements do public agencies in the United States have for effectuating an interruption of wireless service?**..... **17**

*The Interruption of Wireless Services Must Be Assessed Against a Number of Important Laws and Regulations*

*i. Section 151 of the Communications Act*

*ii. Sections 301, 302(b) and 333 of the Communications Act*

*iii. The Pen/Trap Statute – 18 U.S.C. § 3121*

*iv. Sections 201 and 202 of the Communications Act*

*v. Section 20.18 of the Commission's Rules*

*Authority Exists Under Current Law for the Selective Interruption of Wireless Services*

**2. BASES FOR INTERRUPTING WIRELESS SERVICE**

**a. What types of government authorities are most likely to seek intentionally to interrupt wireless service?..... 28**

*Corrections Administrations Require the Selective Interruption of Wireless Services to Combat Contraband Devices in Prisons*

**b. In what kinds of situations would a government authority potentially seek intentionally to interrupt wireless service? How frequently do these situations arise? For how long would service be interrupted in these situations? How rapidly after the threat to public safety has passed can service be restored?..... 29**

*Corrections Administrations Need a Technological Solution to Combat Contraband Devices in Prisons*

*Service Interruption by Managed Access of Combat Contraband Devices in Prisons Can Be Implemented for as Long as Necessary to Address the Problem, but Can Be Effectively and Immediately Terminated Without Collateral Effect if the Problem Abates*

**c. Under what circumstances would an interruption of wireless service likely be effective in protecting public safety? Under what circumstances might interrupting wireless service be ineffective?..... 31**

*Tecore's Managed Access™ Solution Has Been Very Successful at Combating Contraband Devices in the Mississippi State Penitentiary*

*Managed Access Is Effective, However, Only When All Frequencies and Technologies Are Targeted*

**3. RISKS IN INTERRUPTING WIRELESS SERVICE**

**a. What public safety risks arise from intentionally interrupting wireless service? How are the activities of first responders and other emergency personnel and government authorities affected by an intentional interruption of wireless service? How are the activities of consumers affected by an intentional interruption of wireless service?..... 33**

*The Interruption of Wireless Services Risks the Failure to Complete Emergency Calls Unless the Interruption Technology is Nimble and Can Handle Emergency Calling While Preventing Unauthorized Inmate Usage*

*The Interruption of Wireless Services Also Risks The Possibility of Exceeding Its Desired Scope to Affect Communications Not Intended to be Blocked*

**b. What are the potential economic consequences of intentionally interrupting wireless service?..... 35**

*The Wireless Industry Has Not Alleged Any Economic Consequence to the Use of Managed Access to Selectively Interrupt Wireless Service in Prisons*

**c. How do particular circumstances affect the risks that arise from an interruption of wireless service? Are there particular kinds of locations where interruption is especially risky? Are there areas where first responders and other emergency personnel are especially dependent upon commercial wireless service to perform their duties or where consumers are particularly dependent on wireless service? How does the availability of alternative means of communication affect the risks that arise from an interruption of wireless service? Does the interruption of wireless service pose particular risks to persons with disabilities?..... 36**

*Tecore's Solution Has Been Proven at the Rural Parchman Prison and Will Be Further Proven at the Urban Baltimore Metropolitan Transition Center*

**d. What steps could be taken to minimize the risks that arise from an interruption of wireless service? What steps could be taken to narrow the scope of a service interruption?..... 40**

**e. What institutions or officials should be notified of an intentional interruption of wireless service? How and when should they be notified? How and when should the public be notified? Should notifications include the reason for the service interruption?..... 40**

**f. Are there less intrusive ways of protecting public safety than interrupting wireless service? If so, what are they? Under what circumstances are these alternative means likely to be as effective as interrupting wireless service? Should government officials be required to consider alternative means before interrupting wireless service?..... 40**

**g. Are there situations where the risk of interrupting wireless service will always outweigh the benefits?..... 40**

**h. What kinds of liability issues for wireless service providers might be raised by wireless service interruptions?..... 41**

*Liability for Wireless Service Providers Resulting From Voluntary or Involuntary Service Interruptions Is Not Supported by the Law*

**4. SCOPE OF INTERRUPTION**

**a. Can wireless carriers implement a general service interruption, but still ensure that the public can make wireless 911 calls? Would a service disruption that permits wireless 911 calls, but otherwise prohibits voice, text, and data communications, achieve the same purpose as a blanket interruption? Would it pose any unique risks to persons with disabilities? 42**

*Wireless Service Interruptions to Address Prison Cell Phones Can and Should Selectively Block Unauthorized Communications but Permit All Emergency Calling Regardless of Source*

**b. Can wireless carriers implement a service interruption while ensuring that authorized parties would have uninterrupted access to wireless priority service (WPS)?..... 43**

**c. Can wireless carriers implement a service interruption and still provide targeted alerts via the Personal Localized Alerting Network (PLAN) to the public in the affected area?..... 43**

**d. What are the costs and benefits of a service interruption where one or more of wireless 911, WPS, or PLAN are also disrupted?..... 43**

**e. What are the different methods for interrupting wireless service? How do circumstances affect the availability of these methods?..... 43**

**f. How do the effects differ among methods of interruption? Do some methods target a narrower geographic area?..... 43**

**g. What methods of interrupting service would lead to the most rapid restoration of service?..... 44**

**5. AUTHORITY TO INTERRUPT SERVICE**

**a. What processes could ensure that only an appropriate official makes the decision to request an interruption of wireless service? How would such an official be contacted in an emergency situation where time is of the essence?..... 44**

**b. What institutions or officials should be able to review the decision to interrupt wireless service? What process considerations or safeguards should be implemented? How can timeliness of such review be ensured?... 44**

**c. What obligations do or should wireless carriers have to comply with a request by a government official to interrupt wireless service?..... 44**

*Commercial Wireless Carriers Are Not Currently Required to Participate in Wireless Service Interruption as a Means to Combat Contraband Prison Cell Phones*

**d. What steps should be taken to ensure a timely return to full wireless service in the affected area? What institutions or officials should have authority to request a return to full wireless service in the affected area?.. 45**

*The Authority to Operate a System to Selectively Interrupt Wireless Services Should Cease When the Operation of the System is No Longer Needed To Address the Public Safety Concern At Issue*

**e. What procedures should there be to review an interruption after it has occurred?..... 46**

**6. LEGAL CONSTRAINTS ON INTERRUPTING WIRELESS SERVICE**

**a. What sources of legal authority does the Commission have regarding shutdowns of wireless service? What discretion does the Commission have to approve or disapprove shutdowns?..... 46**

*The Commission Has The Authority to Grant Direct Authority to Prison Officials to Operate a Managed Access System in the Event Wireless Carriers Volunteer Spectrum Rights*

*The Commission Should Amend Its Rules to Provide for Access to Spectrum for Managed Access Systems in the Event Carriers Are Unwilling to Act*

**b. Are there circumstances under which a government entity could be construed to have common carrier obligations under the Communications Act due to its relationship with or control over wireless service?..... 49**

*The Operator of a System for Wireless Service Interruption May Be Deemed To Be a Common Carrier Unless Formal Steps Are Taken to Achieve a Different Classification*

**c. What authority does the Commission have to preempt laws and regulations permitting or prohibiting interruption of wireless service? How should the Commission exercise any such authority?..... 50**

*The Proposed Rules Do Not Require the Commission to Preempt Any Law Prohibiting the Interruption of Wireless Service*

**d. What protections do the First Amendment or due process rights provide for users of wireless service? Under what circumstances could an interruption of wireless service violate the First Amendment or due process rights of wireless users? Are there other constitutional protections that should be considered?..... 50**

**e. What protections do the First Amendment, due process, or other constitutional rights afford wireless carriers? Under what circumstances could a forced interruption of wireless service violate the First Amendment, due process, or other constitutional rights of wireless carriers?..... 50**

**f. What provisions of Title II of the Communications Act prohibit or circumscribe an interruption of wireless service, and under what circumstances? To what extent do sections 202, 214, 302a, 333, or other sections of the Communications Act circumscribe the ability of government actors to interrupt wireless service?..... 50**

**g. What state laws prohibit or circumscribe an interruption of wireless service? What authorities do state public utility commissions have to prohibit or circumscribe an interruption of wireless service? Are there circumstances in which approval of a state public utilities commission is necessary before ordering a shutdown?..... 51**

**h.** **To what extent does a public agency's contractual or practical control over wireless service equipment affect the analysis of whether a public agency has the legal authority to interrupt wireless service?..... 51**

**i.** **What is the scope of the Commission's discretion to set policies that affect a public agency's legal authority to interrupt wireless service? To the extent the Commission has not exercised this discretion, should it do so, and in what ways?..... 51**

**CONCLUSION ……..... 51**

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

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| | ) | |
| Wireless Service Interruptions | ) | GN Docket No. 12-52 |

To the Chiefs, Public Safety and Homeland Security
and Wireless Telecommunications Bureaus

## COMMENTS OF TECORE NETWORKS

Tecore Networks ("Tecore"), by its undersigned counsel, hereby submits these Comments in the above-referenced docket addressing issues related to the intentional interruption of wireless service in the interest of public safety.

## INTRODUCTION

### 1. MANAGED ACCESS IS A PROVEN TECHNOLOGY FOR SELECTIVE WIRELESS INTERRUPTION TO BENEFIT PUBLIC SAFETY

Tecore applauds the Commission for initiating this docket and its formal inquiry into the intentional interruption of commercial mobile wireless services when it serves the public interest. Tecore offers herein its comments in those areas of the inquiry identified in Public Notice DA 12-311[1] for which it believes it has the requisite qualifications and experience.[2]

Tecore is in its twentieth year of designing, manufacturing and deploying specialized wireless infrastructure equipment around the world. Over these years, our equipment has served

[1] *Commission Seeks Comment on Certain Wireless Service Interruptions*, GN Docket No. 12-52, *Public Notice*, DA 12-311 (Mar. 1, 2012)(hereinafter "*Public Notice*").

[2] In order to maintain the structure of these comments in line with the structure of the questions laid out by the Commission, as requested in the Public Notice, in those areas where Tecore has no comments to offer, the requisite section heading as outlined by the Commission is followed simply with the legend "COMMENT NOT OFFERED."

the military and intelligence needs of the United States in a variety of difficult environments, including Iraq, Afghanistan and Somalia. Commercially, our systems have provided affordable, flexible and state-of-the-art network capabilities principally to smaller rural and remote areas. Our products have been especially well suited to deployment in specialty applications that fall outside the typical voice and data scenarios of traditional wireless systems.

In this latter regard, we recently pioneered and have a patent pending for one form of selective interruption of wireless service – managed access – to address the growing public safety risk caused by contraband wireless devices in the hands of prison inmates who are using the devices to conduct dangerous criminal activity from within prisons. Tecore was the first to use standard, industry-compliant wireless network equipment to deploy a wireless service umbrella covering restricted prison facilities underneath the existing wireless networks footprints in the prison area. The service umbrella provided by the Tecore equipment selectively manages the access of wireless devices to those existing wireless networks – and thereby prevents contraband devices from completing voice, text and data transactions on the networks. Tecore's Managed Access™ solution has been increasingly successful in preventing dangerous prison inmates from gaining access to wireless communications within prison walls and utilizing the access for illegal – and in some cases deadly – purposes.

## 2. A SUCCESSFUL MEANS TO DEFEAT CONTRABAND DESERVES A BETTER REGULATORY FRAMEWORK

To be a comprehensive solution to the problem of contraband devices, a managed access system must insert its authentication and denial capability between *all* contraband devices and *every* commercial wireless network that can serve them within the prison grounds. As a result, a managed access system must operate within all of the radio frequency bands across 2G, 3G and 4G evolutions (*e.g.*, 700, 800, 1900 and 2100 MHz) and radio technologies (*e.g.*, GSM, CDMA,

iDEN, etc.) on which all commercial carriers providing a usable wireless signal to the prison are operating. Under current FCC rules, managed access systems must operate as a lessee of spectrum from the commercial wireless licensees in the prison area. The participation of the commercial wireless operators is voluntary, and prison officials must obtain the voluntary cooperation of *all* wireless carriers in order to operate a comprehensive managed access solution at their facilities. Any carrier that elects not to provide spectrum rights will leave a "hole" in the interdiction umbrella which can and will be quickly be exploited by inmates.

No regulation currently prevents any wireless carrier from opting *not* to permit interdiction within its spectrum. Similarly, nothing prevents a carrier from making spectrum available only under terms and conditions that are unreasonable or unworkable, or which undermine the economic feasibility of managed access. The inadequacy of this regulatory environment already is evident. Despite the success of managed access at the Mississippi State Penitentiary at Parchman, Mississippi, for example, the deployment of managed access to Mississippi's two other state prisons has been frustrated by the refusal of certain wireless carriers to provide spectrum.

The foregoing is not to suggest that there has not been good cooperation from the commercial wireless industry as a whole during the development of managed access by Tecore. Indeed, a key element in the initial success of Tecore's wireless interdiction solution has been the active and cooperative participation of the major commercial wireless carriers. Five major commercial wireless carriers – AT&T, C-Spire, Sprint Nextel, T-Mobile and Verizon – each have supported the deployment of managed access systems and have volunteered spectrum rights

for the testing and deployment of these systems.[3] The Cellular Telecommunications Industry Association ('CTIA"), speaking on behalf of the entire wireless industry, has endorsed managed access as its preferred technology solution for the interdiction of contraband devices.[4]

However, with the most recent Mobile Wireless Competition Report identifying over 100 nationwide, regional and smaller commercial wireless operators currently providing some form of facilities-based cellular or cellular-like service in the United States,[5] it is unreasonable to expect that the issues already encountered in Mississippi with the desired expansion of its highly-successful managed access solution to the state's other corrections units may not become a major stumbling block to the successful deployment of managed access solutions nationwide.

---

[3] In response to the Notice of Inquiry issued by the National Telecommunications and Information Administration ("NTIA") in 2010 seeking public comment on alternative wireless interruption and detection technologies, AT&T stated that "[m]anaged network access technology offers the most effective method for preventing contraband cell phone use while also protecting the important communications made by public safety and authorized consumers" and added that "managed network access solutions should form the foundation of NTIA's plans to prevent contraband cell phone use in prisons. National Telecommunications and Information Administration, *Preventing Contraband Cell Phone Use in Prisons*, Notice of Inquiry, 75 Fed. Reg. 26733 (May 12, 2010) ("*NTIA NOI*") Comments of AT&T Inc. (Jun. 11, 2011), at 10-11, 14 http://www.ntia.doc.gov/files/ntia/comments/ 100504212-0212-01/attachments/ATT_Filing_-_Jammers_ Comments_-_6-11-2010.pdf). In its comments, Sprint Nextel offered that managed access (together with device detection) "offer the best potential solution to the problem." *NTIA NOI*, Comments of Sprint Nextel Corporation (Jun. 11, 2011), at 10-11, 14, http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/Sprint_Jammer_Comments_-_061110final.pdf. T-Mobile stated in its comments that "[m]anaged access systems are a preferable solution for preventing the use of contraband cell phones within prisons because they can effectively prevent unauthorized communications without disrupting legitimate users or emergency calls and also provide additional helpful intelligence gathering capabilities. *NTIA NOI*, Comments of T-Mobile USA, Inc. (Jun. 11, 2011), at 8 http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/T-Mobile__NTIA_Jammers_ Comments.pdf. "Managed access systems," Verizon stated in its comments, "are far superior to jamming systems for controlling and preventing contraband cell phone use in prisons" and encouraged NTIA to "recommend managed access as the superior technology for preventing contraband cell phone use in prisons…." *NTIA NOI*, Comments of Verizon Wireless (Jun. 11, 2011), at 11, http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/VZW_jamming_NOI_comments_6-11-10.pdf).

[4] *NTIA NOI*, Comments of the Cellular Telecommunications Industry Association (Jun. 11, 2010), at 5, 12-13, http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/CTIA100611_Contraband_Use_of_Phones_in_Prisons_NOI_Comments_FINAL_FILED.pdf. The Wireless Communications Association International also publicly supported the deployment of managed access. Letter from Susan Polyakova, Vice President, Wireless Communications Association, International to Marlene H. Dortch, Secretary, Federal Communications Commission, WT Docket No. 09-30, at 1 (July 30, 2009).

[5] Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, including Commercial Mobile Services, WT Docket No. 10-133, *Fifteenth Report*, 26 FCC Rcd 9664, 9693-95 (2011).

With serious national public safety risks resulting from the increasing availability of unauthorized wireless communications to inmates, it is unacceptable that any carrier licensed by the Commission to operate on the public airwaves should be permitted to block the deployment of a proven technological solution to the problem and leave corrections officials with no means to employ an effective technology solution. In light of the paramount importance to public safety and the administration of justice represented by the effective control of illegal communications by inmates, it is squarely in the public interest for the Commission to create a means by which managed access systems may be deployed even in the absence of wireless carrier cooperation. Given the significant cost of installing and operating a technology solution like managed access, it is difficult for prison systems to justify such expenditures if they are not assured of stable, long term access to spectrum.

## COMMENTS

### 1. PAST PRACTICES AND PRECEDENTS

#### a. Under what circumstances have public agencies in the United States considered or effectuated interruptions of wireless service for public safety reasons?

*Contraband Wireless Devices and the Criminal Activity They Are Used to Conduct Warrant the Selective Interruption of Wireless Services in Corrections Facilities*

In general, the possession and use of cell phones and other wireless devices by prison inmates in the United States is prohibited by law or by prison rules. Persons visiting a prison likewise are generally prohibited from introducing a wireless device into the corrections facility.[6]

[6] *See, e.g.,* U. S. Department of Justice, Federal Bureau of Prisons, *Legal Resource Guide to the Federal Bureau of Prisons 2008,* http://www.bop.gov/ news/PDFs/legal_guide.pdf, at 30 ("Third-party or other alternative call arrangements are not permitted, thus limiting the opportunity for inmates to use the phones for criminal or other inappropriate purposes. Inmates are not permitted use of cellphones or electronic communication devices. Any such possession or use is grounds for disciplinary action and possible criminal prosecution."); New York State Department of Correctional Services, *Handbook for the Families and Friends of New York State DOCS Inmates* (Dec. 2007), http://www.docs.state.ny.us/FamilyGuide/FamilyHandbook.pdf, at 10-11 ("The introduction of

The possession of cell phones by prison staff is also frequently prohibited or strictly controlled.[7]

A growing list of states have enacted legislation to bolster existing "no cell" policies in prisons by criminalizing the introduction of contraband devices into corrections environments and mandating severe penalties for violations.[8] At the Federal level, the Cell Phone Contraband

---

contraband to the facility is ABSOLUTELY PROHIBITED. Contraband is defined as … [a]nything that is not specifically authorized to be possessed by an inmate in a state correctional facility according to the rules of the Department or local rules of the facility. (Cell phones, alcohol and money are among the items inmates are not permitted to possess.).

[7] *See, e.g.*, Public Safety and Homeland Security Bureau Workshop on Contraband Cell Phone Use in Prison, Comments of Jon Ozmint, South Carolina Department of Corrections (Sept. 30, 2010)("*Ozmint Comments*"); *see* Transcript of Public Safety and Homeland Security Bureau Workshop on Contraband Cell Phone Use in Prison http://www.fcc.gov/pshs/docs/summits/contraband-cell-use-transcript.pdf ("*Workshop Transcript*") at 4, 37 ("[T]here are no legal cell phone calls on prison property in South Carolina. … In some states there's such a thing as a legal cell phone call made from prison property. I concede that. But in some states there is no such animal."). *But see* Public Safety and Homeland Security Bureau Workshop on Contraband Cell Phone Use in Prison, Comments of Christopher Epps, Mississippi Department of Corrections (Sept. 30, 2010)("*Epps Comments*"); *see Workshop Transcript* at 47-48 ("[The Mississippi State Penitentiary] is 18,000 acres. We even have staff that live on the grounds of the penitentiary. We lease out 8,000 of those acres. We farm the rest of it. So we have farmers on the ground. … [W]e put some of those individuals who live on the grounds that have cell phones we put them in the system. The superintendent of the prison is in the system. Obviously, I'm in the system.")

[8] Among the examples of state legislative activity in this area are the following:

- ***California.*** In October 2011, California passed a statute making it a misdemeanor to smuggle cell phones into California prisons. The law carries a punishment of six months in jail and up to $5,000 in fines for each device. Inmates found with contraband phones will lose time credits they may have earned for good behavior and may have to serve their full sentences as a result. Cal. Pen. Code § 4576. At the same time, the California Governor signed Executive Order B-11-11, which ordered the California Department of Corrections and Rehabilitation to develop and deploy a cost-efficient system to interrupt unauthorized cellular transmissions at the state's prisons in a manner consistent with Federal law, and to work with other state agencies to accelerate the process for procurement of a system to interrupt unauthorized cellular transmissions. Cal. Exec. Order B-11-11 (Oct. 6, 2011).
- ***Illinois.*** In 2009, Illinois amended its Criminal Code to provide for enhanced penalties if a defendant at the time of the commission of an offense is either a pre-trial detainee or is serving a sentence at a penal institution and obtains or uses a communications service without authorization. 720 Ill. Comp. Stat. § 5/16-19, 16-20.
- ***Maryland.*** In Maryland, a series of bills are currently under consideration by the House of Delegates regarding contraband devices in the state's prisons. House Bill 587 increases penalties for the possession of a cell phone or other device by an inmate and for delivering or attempting to deliver a cell phone to an inmate. An inmate caught with a device would face a felony sentence of five years. Anyone caught delivering a device to an inmate would be subject to a misdemeanor sentence of up to three years on a first offense and a felony sentence of up to five years on subsequent offenses. Senate Bill 669 and companion House Bill 1086 would take away good-time credit permanently for inmates caught with a prohibited device. [cite needed]
- ***Michigan.*** Senate Bills 551 and 552, currently under consideration by the Michigan legislature would expand the provisions of the 2006 law prohibiting individuals in the state from supplying unauthorized wireless devices to inmates in state prisons to criminalize the possession of such unauthorized devices by

Act was signed into law in 2010. The Federal statute classifies cell phones and wireless devices as contraband material and prohibits the use or possession of such contraband in Federal prisons. Anyone providing or attempting to provide an inmate with a cell phone may face up to one year of imprisonment.[9]

Despite all of these efforts by corrections officials and lawmakers, the nation's prisons, jails and other correctional facilities have faced, in recent years, an increasingly uncontrollable epidemic of contraband wireless devices in prisons. The increasing availability of unauthorized and unmonitored wireless communications to dangerous inmates presents a substantial risk to public safety. Contraband wireless devices increasingly are the means by which inmates coordinate illegal activity outside the prisons. In the most extreme cases occurring to date, the illegal activity conducted by cell phone has included the murder of prison officials, public officials and witnesses.[10]

---

the inmates and extend the same restrictions to local corrections facilities throughout the state. Mich. Comp. Laws 800-263(a).

- ***Oklahoma.*** In 2009, Oklahoma approved a measure to strengthen its existing statute regarding the prohibition of wireless devices in prisons and other secured areas. Under the amended law, it is a felony (it had previously been a misdemeanor) for any person to bring into any secure area of a jail or state penal institution or other secure place where prisoners are located any electronic device capable of sending or receiving any electronic communication. Any infraction of the statute is punishable by imprisonment for up to two years or by a fine of up to $2,500. 57 Okl. St. Ann. § 21.

[9] 18 U.S.C. § 1791.

[10] *See, e.g., Special Report: Inmate Cell Phone Use Endangers Prison Security and Public Safety*, Office of the Inspector General, State of California (May 2009), http://www.oig.ca.gov/media/reports/BCI/Special_Report_of_Inmate_Cell_Phone_Use.pdf, at 1 ("According to numerous California Department of Corrections and Rehabilitation (Department) officials, the possession of cell phones and electronic communication devices by California's inmates is one of the most significant problems facing the Department today."); Department of Justice, Office of Justice Programs, National Institute of Justice, *Cell Phones Behind Bars* (Dec. 2009), http://www.ncjrs.gov/pdffiles1/nij/227539.pdf; Public Safety and Homeland Security Bureau Workshop on Contraband Cell Phone Use in Prison, Comments of Thomas Kane (Sept. 30, 2010); *see Workshop Transcript* at 20 *et seq*. Briefing Sheet, *Putting An End to Illegal Cell Phone Use in Prisons*, Public Safety and Homeland Security Bureau ("*Briefing Sheet*")("Contraband cell phones have been used by inmates to arrange the murder of witnesses and public safety officers, traffic in drugs, and manage criminal enterprises. This illegal practice jeopardizes the safety of America's communities and public safety officials.")

Until recently, prison officials largely combated the problem by physical search and seizure methods, in an effort to locate and remove unauthorized devices from prisons. Prison administrators have begun to recognize that this manpower-intensive program of confiscation – requiring the use of prison facility and inmate, staff and visitor searches and specialized equipment and search animals – has had limited success in stemming the availability and use of contraband devices and has not been particularly cost effective. Corrections officials have clamored for technology that can effectively address the problem.[11]

In December 2009, the United States Congress inserted language in the Conference Report to the Department of Commerce Fiscal Year 2010 Appropriations tasking the NTIA, in coordination with the Commission as well as the Federal Bureau of Prisons and the National Institute of Justice, to investigate and evaluate how wireless technologies might be utilized for law enforcement and corrections applications in Federal and state prisons.[12]

In its Notice of Inquiry in the matter, comments were submitted by corrections departments, wireless carriers, equipment vendors (including Tecore) and other interested parties

---

[11] *NTIA NOI*, Comments of the California Department of Corrections and Rehabilitation (Jul. 7, 2010), http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/CA_NTIA_Response_Letter.pdf ("In April of 2009 we implemented a pilot program at one of our institutions that consisted of canines trained to detect cell phones. … Additionally, we have increased searching of inmates, visitors, and staff specifically to identify and seize contraband cell phones. … However, these are only stop-gap measures and more comprehensive solutions are needed."); *Epps Comments* at 31 **("**We … search staff. We search inmates. We have dogs trained to find cell phone. In addition to that we prosecute staff and terminate them and we prosecute civilians. But after all of that we were still having problems with cell phones getting in through various means…."); *NTIA NOI*, Comments of the South Carolina Department of Corrections (Jun. 10, 2010), http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/S.C._Corrections_Department_-_Contraband_Cell_Phone_Comments .pdf, at 2 ("*South Carolina DOC Comments*") ("While cell phones are contraband in prison, contraband can get past even the best detection systems. X-ray scanners, metal detectors, drug and bomb dogs, and the best of search techniques are all creations of human ingenuity and they can all be defeated by human ingenuity.")

[12] *See e.g.*, H.R. Conf. Rep. No. 111-336 (2009), Division B, Title I, at 619 ("The conferees are concerned with the increased smuggling of contraband cell phones into State and Federal prisons and the use of such devices by inmates to orchestrate prison-breaks, conduct illegal activity, and harass or intimidate judges, lawyers or former victims."); *see also generally* S.1749, Cell Phone Contraband Act of 2010, 111th Cong. (2010); S.251, Safe Prisons Communications Act of 2009, 111th Cong (2009)("*Safe Prisons Act*"); H.R.560 Safe Prisons Communications Act of 2009, 111th Cong (2009).

on the three radio frequency (RF)-based technologies which could interdict contraband devices[13] that were pinpointed by NTIA for further evaluation – including managed access. In December 2010, the NTIA issued its summary report in the matter, and made several key observations about the effectiveness of managed access in addressing the problem and the prevention of collateral impacts on authorized commercial communications outside prisons and emergency 911 calling.[14]

The Commission, especially its staff in the Wireless Telecommunications and Public Safety and Homeland Security Bureaus, the Office of Engineering and Technology, and the Office of General Counsel, early on recognized the growing problem of the unauthorized possession and use of wireless devices by prison inmates, and actively supported and

---

[13] NTIA recognized that "contraband devices" may include "any wireless, portable device that is available to the public on a subscription or prepaid basis for delivering voice and/or data services such as text messages" and could include "phones operating within the Cellular Radio Service in the 800 MHz bands; broadband Personal Communications Services (PCS) in the 1.9 GHz bands; the Advanced Wireless Services (AWS) in the 1.7 GHz band; Specialized Mobile Radio (SMR) services in the 800 and 900 MHz bands; and any future mobile wireless devices that plan to operate in bands such as the 700 MHz band." *NTIA NOI*, 75 Fed. Reg. 26733 n.1.

[14] Among the observations made by the NTIA were that managed access (1) can prevent prisoners from communicating by cell phone with people outside the prison, while at the same time permit authorized users to pass through to the network and handle all 911 calls, (2) addresses the licensed spectrum bands commercially available today, but can be upgraded to cover Long Term Evolution ("LTE") and 700 MHz band development, as any viable solution must be comprehensive and address the growing diversity of commercial telecommunications technologies and frequencies available to the public – including also AWS, WiMAX, General Mobile Radio, satellite, Wi-Fi and Bluetooth devices, (3) does not violate the Communications Act if the FCC issues the proper authorizations and the users comply with the terms of those authorizations, (4) requires structured coordination and cooperation between a managed access system vendor and the wireless service providers in the affected area, and (5) can be potentially deployed at no cost to the prison authority, based on a separate arrangement between the managed access and pay phone service vendors. In general, comments asserted that some form of service interruption is a promising solution to the contraband problem, and that managed access is not only a viable – but a preferred – solution. National Telecommunications and Information Administration, *Contraband Cell Phones in Prisons: Possible Wireless Technology Solutions* (Dec. 29, 2010) at 19-26 ("*NTIA Report*"). CellAntenna Corporation, a major proponent of jamming technology, asserted in its comments in the proceeding that prohibiting the access of prison cell phones to the commercial cellular networks "would solve 90-95% of all illegal communications within a prison." *NTIA NOI*, CellAntenna Corp. Answers to the NTIA Questions and Comments on Cell Phones and Prisons (Jun. 9, 2010) at 4 ("*CellAntenna Comments*"). Major commercial carriers AT&T and T-Mobile both recognized in their comments that the viability of managed access for controlling contraband cell phone use. *NTIA NOI*, Comments of AT&T Inc. (Jun. 11, 2010) at 10-14; *NTIA NOI*, Comments of T-Mobile USA, Inc. (Jun. 11, 2010) at 7-8. Global Tel*Link, the inmate telephone service company which operates the Tecore Managed Access™ solution at Parchman, Mississippi, for the Mississippi Department of Corrections, contended in its comments to the NTIA that managed access is the frontrunner for technology of choice from the wireless industry's point of view. *NTIA NOI*, Comments of Global Tel*Link Corp. (Jun. 11, 2010) at 5 ("*GTL Comments*").

affirmatively facilitated the early deployment of managed access technology to address the critical need of the corrections community.[15] The proactive efforts by Tecore and the Commission lead to impressive results. The Tecore solution went live at the Mississippi State Penitentiary in August 2010, and in its first 60 days of operation had already blocked over 365,000 call and text message attempts – or 6,000 attempts per day on average. By February 2012, over 2 million calls and text messages had been prevented in this single facility.[16] The

[15] *See, e.g., Briefing Sheet, supra.* ("The FCC has made it a top priority to put an end to illegal cell phone use by inmates in prisons.")

[16] Mississippi Department of Corrections, THE RESOURCE (October 2010), at 7, http://www.mdoc.state.ms.us/News_Letters/2010NewsLetters/October2010.pdf; "Keeping Cell Phones Out of Jail Cells," WIRELESS, Apr. 21, 2011, http://www.businessweek.com/_magazine/content/11_18/b4226042114325.htm. As a result of the successful deployment at Parchman, Mississippi Corrections Commissioner Christopher Epps endorsed the technology as the best solution to the problem of contraband wireless devices in prisons stating "I haven't seen anything better than managed access to deal with illegal cell phones" and calling managed access "the future for prisons." *Id.*

success of managed access in Mississippi has generated tremendous interest nationwide[17] and has led to a number of requests for proposal for managed access systems.[18]

**b. What are relevant examples of foreign governments considering or effectuating interruptions of wireless service for public safety reasons? What laws or policies do foreign states have regarding interruption of wireless service for purposes of protecting public safety?**

*Foreign Governments Have Permitted Wireless Interruptions Not Only for Public Safety but to Achieve a Variety of Other Goals*

Like the United States, a number of countries have permitted or are considering the use of technology for the controlled interruption of wireless services in and around prisons and other correctional facilities in the interest of public safety – including Brazil, France, Germany, India,

[17] In a recent survey, the Association of State Corrections Administrators conducted a blind poll of corrections departments around the United States on the subject of managed access technology and found widespread support for the solution. Comments included:

- "The *advantages* of this system are abundant…."
- "This is *perfect* for correctional facility use…."
- "It appears to be the *best industry option* available for mitigating the use of illegal/contraband cell phones in correctional institutions…."
- "Of all of the available technologies that we have reviewed, the *most viable option* to stop the illegal trafficking and use of cellular telephones by our offender populations is through managed access…. All other means of control are either not as effective, do not work as billed, are labor intensive or illegal under the FCC to operate...."
- "The MA DOC believes a managed access system is the *best way* to prevent inmates from accessing carrier networks using cell phones…."
- "WVDOC views managed access technology *more favorably* than other detection technologies…."
- "The general impression is that managed cell phone access is the *best thing* on the market to control cell phones in the correctional setting…."

Association of State Corrections Administrators, Cell Phone Managed Access Survey Comments (Jun. 2010), at 3, 5, http://www.asca.net/ system/assets/attachments/3364/B2._Cell_Phone_Managed_Access_ Survey_Comments-2.pdf?1312550012), at 1-4, 6-7 [emphasis added]("*ASCA Survey*").

[18] *See, e.g.*, Maryland Department of Public Safety and Correctional Services, *Request for Proposals (RFP) – Cell Phone Managed Access Services* (Sep. 27, 2011), http://www.dpscs.state.md.us/publicservs/procurement/Q0012011/RFP.pdf and California Technology Agency, Inmate Ward Telephone System And Managed Access System Services (Jul. 7, 2011), http://www.bidsync.com/DPX?ac=view&auc=18105 50).

Iran, Ireland, Italy, Mexico, New Zealand, Sweden and the U.K. While laws and regulations regarding the interruption of wireless services vary greatly across the world, many countries prohibit, in one form or another, the interruption of wireless services by use of radio signal jamming technology as does the United States.[19] Despite a similar baseline prohibition on jamming, however, unlike the United States, the countries listed above have permitted or are considering the use of jamming technology to control contraband wireless devices in prisons. On the other hand, some countries have considered and rejected the use of jammers to control contraband cell phones in prison. Australia, for example, twice considered and rejected a modification of their general ban on jamming to permit jammers to be used in prisons.[20]

Around the world, news reports indicate that governments have employed wireless service interruption in a wide variety of scenarios – for reasons of public safety reasons but also for a range of non-public safety goals, including the following examples:

- ***Law Enforcement and the Military***. In has been reported that the U.K.'s London Metropolitan Police employs covert radio service umbrellas in selected instances to intercept,

[19] Although the Commission's public notice inviting comment specifically requested that comments not discuss jamming, it is discussed here only to be illustrative of the form wireless interdiction has often – but not always – taken outside the United States. Jamming is prohibited under Section 333 of the Communications Act of 1934, as amended, which states that "[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government." 47 U.S.C. § 333. Among the countries prohibiting radio signal jamming in whole or part are Australia, Brazil, Canada, Germany, Iran, Ireland, Italy, Japan, Mexico, New Zealand, Norway, Pakistan, Poland, Sweden, Turkey and the United Kingdom.

[20] Australia imposed a general ban on jamming technology in 1999. In 2003, the former Australian Communications Authority considered, and rejected, a request to exempt prisons from the jamming ban. After corrections officials in the country renewed its request for a jamming solution to contraband mobile phones in prisons, the Australian Communications and Media Authority undertook a fresh review of the issue and again refused to create an exemption to the ban for corrections facilities. *See* Radiocommunications (Prohibition of PMTS Jamming Devices) Declaration 2011, F2011L00346 (Feb. 18, 2011), http://www.comlaw.gov.au/Details/F2011L00346; Review of Mobile Phone Jammer Prohibition, Issues for Comment (IFC) 02/2010 (Feb. 2010), http://www.acma.gov.au/WEB/STANDARD/ pc=PC_312026.

and in some cases interrupt, wireless communications.[21] Law enforcement agencies and/or the military are permitted to deploy jamming technology in the course of their mission in Canada, Iran, Italy, Mexico, New Zealand, Norway and Turkey.[22] In Canada, law enforcement agencies are required to obtain specific approval prior to any use of jammers.[23]

- ***Government Institutions.*** In India, jamming technology has been installed to prevent the use of wireless devices by any persons, including legislators, in the houses of the Legislative Assembly and Legislative Council in order to limit interruptions to legislative work.[24]

- ***Educational Institutions.*** In Uzbekistan, mobile Internet and messaging services (but not voice services) have been interrupted nationwide during the taking of nationwide university entrance examinations in an effort to prevent cheating.[25] More localized interruption by jamming during scholastic exams reportedly has been employed or considered in China, India and Iran.[26]

---

[21] Kim Zetter, *UK Cops Using Fake Mobile Phone Tower to Intercept Calls, Shut Off Phones*, WIRED (Oct. 31, 2011), http://www.wired.com/threatlevel/2011/10/datong-surveillance/. Cell phone jammers generally are prohibited under Section 8 of the Wireless Telegraphy Act of 2006. Wireless Telegraphy Act 2006, § 8. Military and government departments, however, may deploy jammers after getting authorization from the U.K.'s Office of Communications. *See* Office of Communications, Mobile phone jammers and cellular enhancers, http://stakeholders.ofcom. org.uk/enforcement/spectrum-enforcement/jammers/.

[22] *See infra* n.19, 21; Mike Elgan, *Should Cell Phone Jamming be Legal?*, PCWORLD (Feb. 28, 2009), http://www. pcworld.com/businesscenter/article/160420/should_cell_phone_jamming_be_legal.html ("*PCWorld*").

[23] Section 9(1)(b) of the Radiocommunications Act of Canada prohibits the interference with or obstruction of radio communications without a "lawful excuse" and Section 4(1) of the Act prohibits the installation, operation or possession of a radio apparatus without a radio authorization. Radiocommunication Act, R.S.C., 1985, c. R-2 §§ 4(1), 9(1)(b). The Canadian government will issue an "Exemotion Order" to these restrictions for law enforcement in specific circumstances. *See* Radiocommunication Act (subsection 4(1) and paragraph 9(1)(b)) Exemption Order (Security, Safety and International Relations), No. 2010-1, http://www.gazette.gc.ca/rp-pr/p2/2010/2010-03-03/html/sor-dors29-eng.html.

[24] S.A. Hemantha Kumar, *Go-ahead granted for new jammers*, EXPRESSBUZZ (Mar. 10, 2012), http://expressbuzz. com/states/karnataka/go-ahead-granted-for-new-jammers/371232.html, Churches installing cell phone jammers, MSNBC.COM (Oct. 18, 2004), http://www.msnbc.msn.com/id/6272681/ns/technology_and_science-wireless/t/ churches-installing-cell-phone-jammers/#.T2IorXlnDOM (hereinafter "*MSNBC.com*").

[25] Uzbekistan 'halts mobile Internet, SMS' for exam day, PHYSORG.COM (Aug. 2, 2011), http://www.physorg.com/ news/2011-08-uzbekistan-halts-mobile-internet-sms.html.

[26] *PCWorld, supra,* at n.18; *MSNBC.com, supra* at n.20.

- ***Religious Sites.*** Jammers apparently have been deployed in churches in Italy and Mexico to protect the integrity of religious services.[27] India also has reportedly used jamming technology in and around religious sites.
- ***Health Care Facilities.*** Jamming technology also apparently has been used in Italy and Mexico to interrupt wireless services in and around hospitals. Although no rationale could be found for such interruption, presumably the policy goal was the control of nuisance and noise, and possibly for the control of radio interference with the proper operation of medical equipment.
- ***Performance Venues.*** According to press accounts, France, Italy and Japan all have permit jamming in movie theaters, concert halls and other performance venues, likewise presumably for the control of nuisance and noise. In France and Italy, such use may not interfere with mobile emergency calling. In Italy, such use also may not interfere with heart pace makers or other medical devices. In Japan, a government-issued license is necessary prior to this type of jamming.
- ***Research Facilities.*** India, Iran and Pakistan reportedly have permitted jammers to be used in and around public libraries, again presumably for nuisance and noise control.
- ***Financial Institutions.*** In both Mexico and Pakistan, jamming has been employed to protect banks. The rationale provided by the Pakistanis was that the radio umbrella would prevent the remote detonation of bombs which can threaten criminal targets such as banks.
- ***Protection of Sensitive Information.*** It has been reported that in Italy, the use of jamming technology has been permitted in and around buildings where commercial activity is taking place in order to inhibit the leakage of sensitive information. Such use again reportedly

[27] *Id.*

may take place only provided that emergency calling and medical devices are not interfered with or interrupted.

- ***Personal Use.*** In Japan, the purchase and use by the public at large of short range jammers is permitted, and that personal "interruption zones" in homes or offices are legal. Similarly, low power jamming devices are permitted to be used in Poland on one's property provided the use causes no interference with third party communications.

- ***Social Control.*** During the 2009-2010 Iranian election protests, Iranian police reportedly used cell phone and Bluetooth jamming technology to thwart communication among the protesters.[28] Similarly, in Egypt during the 2010 peaceful "revolution," the Mubarak government reportedly shut down wireless towers and Internet services in order to frustrate the efforts of protesters. It has been reported that in Afghanistan the Taliban rebels have begun using the interruption of wireless service as a means of intimidating the populace and undermining the legitimate Afghan government.

**c. What are examples of wireless networks actually being used to put the public's safety at risk? Could interruption of wireless service have mitigated these harms? How would such interruptions have mitigated these harms?**

*Inmates Have Increasingly Leveraged the Availability of Wireless Services to Obtain Cell Phones and Use Them to Engage in Dangerous Criminal Activity*

The Commission is by now quite familiar with the threat to public safety resulting from contraband wireless devices in the hands of prisoners. The threat comes not from inmates engaging in normal communications with family and friends, but rather from the increasing use

[28] Iran blocks TV, radio and phones – but web proves more difficult, THE GUARDIAN (Jun. 15, 2009), http://www.guardian.co.uk/technology/2009/jun/15/iran-jamming-technology-tv-radio-internet; Poll results prompt Iran protests, AL JAZEERA (Jun. 14, 2009), http://www.aljazeera.com/news/middleeast/ 2009/06/2009613172130303995.html.

of the wireless access to plan and conduct criminal activity from behind prison walls.[29] The Public Safety and Homeland Security Bureau has already publicly recognized that "[t]he use of cell phones by prisoners to carry out criminal enterprises is a significant problem across the nation *and demands effective and prompt remedies*."[30]

While there are clear examples of the use of contraband devices to engage in or further criminal activity, no records exist on the scale of the problem. In this regard, however, the following statistics might illuminate the frequency with which wireless devices are utilized in criminal activity overall in the United States. According to the most recent Wiretap Report issued by the Administrative Office of the U.S. Courts, over 95% of all law enforcement wiretaps authorized by Federal and state courts in this country in 2010 involved wireless devices. The number of wireless surveillances authorized has more than quadrupled over the last ten years, to a record high of 3053 in 2010. Since 2000, authorized wiretaps have resulted in ***over 68,000 arrests and over 28,000 convictions***. The vast majority of authorized wiretaps are related to the illegal drug trade. Clearly, the illegal activity being conducted or furthered by inmates who gain access to contraband devices must be significant. It is hard to fathom that simply the desire to speak to loved ones on a personal cell phone rather than the telephones made available

---

[29] *See, e.g.*, Jessica Mulholland, *Combating Contraband Cell Phones in Prisons*, GOVERNED (Nov. 16, 2010), http://www.governing.com/topics/technology/Combating-Contraband-Cell-Phones-in-Prisons.html; Brent Jones, *Former correctional officer pleads guilty to supplying drugs, cell phone to inmate*, THE BALTIMORE SUN (Jun. 7, 2010), http://articles.baltimoresun.com/2010-06-07/news/bs-md-ci-correcitional-officer-20100607_1__correctional-officer-cell-phone-probation-officer; Vince Beiser, *Prisoners Run Gangs, Plan Escapes and Even Order Hits With Smuggled Cellphones*, WIRED (May 22, 2009), http://www.wired.com/politics/law/magazine/17-06/ffprisonphones).

[30] Public Notice, *Public Safety and Homeland Security Bureau Releases Updated Agenda for Workshop/Webinar on Contraband Cell Phone Use in Prisons* (Sept. 24, 2010)[emphasis added].

by prisons for legal use by inmates is what propels inmates to pay exorbitant amounts for smuggled devices.[31]

*Managed Access Has Successfully Defeated Contraband Wireless Devices and Mitigated the Public Safety Risk*

The good news is that it has now been proven by experience that the interruption of wireless services utilizing Tecore's system at correctional facilities renders contraband wireless devices at those location ineffective to conduct any form of communication, however malicious. As mentioned above, in its first 60 days of operation at the Mississippi State Penitentiary, the managed access system blocked over 365,000 call and text message attempts – or 6,000 attempts per day on average. By February 2012, over 2 million calls and text messages had been prevented in this single facility.[32]

**d. What existing policies do public agencies in the United States have for determining whether a service interruption is proper? What existing policies or agreements do public agencies in the United States have for effectuating an interruption of wireless service?**

*The Interruption of Wireless Services Must Be Assessed Against a Number of Important Laws and Regulations*

*i. Section 151 of the Communications Act*

Section 151 of the Communications Act creates the Federal Communication Commission for the purpose, inter alia, of "regulating interstate and foreign commerce in communication by wire and radio . . . for the purpose of promoting safety of life and property through the use of

[31] Inmates will pay hundreds or thousands of dollars to get their hands on contraband phones, and corrupt guards and others can make many thousands of dollars by smuggling the devices into corrections facilities. *See, e.g.*, Julie Small, *California bill to rid prisons of smuggled cell phones shelved over costs*, SOUTHERN CALIFORNIA PUBLIC RADIO (Apr. 22, 2011), http://www.scpr.org/news/2011/04/22/26059/california-bill-to-rid-prisons-of-smuggled-cell-ph/.

[32] Mississippi Department of Corrections, THE RESOURCE (October 2010), at 7, http://www.mdoc. state.ms.us/ News_Letters/2010NewsLetters/October2010.pdf; "Keeping Cell Phones Out of Jail Cells," WIRELESS, Apr. 21, 2011, http://www.businessweek.com/ magazine/content/11_18/b4226042114325.htm.

wire and radio communications."[33] Accordingly, in assessing either existing or future regulations to effectuate the interruption of wireless services, the Commission must ensure that the operation of such communications devices promotes the public safety. If not, then the Commission would have the authority under Section 151 to restrict the operation of such services when they do not promote the public safety and to sanction the use of technologies that promote the safe use of the national communications system.

*ii. Sections 301, 302(b) and 333 of the Communications Act*

Section 333 of the Communications Act offers a critical yardstick against which any potential service interruption must be measured.[34] Section 333, of course, provides that "[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under [the Communications Act] or operated by the United States Government." Prior FCC decisions reflect that interruption technologies must be assessed as well against Sections 301 and 302(b) of the Communications Act.[35]

The Commission has concluded that some forms of interruption technology (*e.g.*, jamming) are prohibited by Sections 333, as well as Section 301 and 302(b), and that it lacks any

[33] 47 U.S.C. § 151.

[34] The Commission noted in *In re Imposition of Forfeiture Against Capitol Radiotelephone Inc., et al.*, 9 FCC Rcd 6370, 6380 (ALJ 1994) *aff'd* 11 FCC Rcd 2335 (1996)(hereinafter "*Capitol Radiotelephone*"), that the "express language" of the provision makes it clear that the target of the law is any "deliberate act with actual intent to cause interference to a licensee's transmissions." The FCC asserted that its conclusion is supported by the legislative history of the section, citing H.R. Rep. No. 101-316, at 13 (1989)(hereinafter "*Section 333 Legislative History*"), which it asserted makes clear that the purpose of the statute is to prohibit "actions that are expressly designed to cause interference." *See also In re Jack Gerritsen*, 20 FCC Rcd 19256, 19259 (EB 2005). FCC decisions distinguish intentional interference, which is prohibited and which will subject the offender to sanction, from occasional unintentional interference incidental to operating in a saturated radio environment. *See, e.g., In re Cordell Engineering, Inc.*, 14 FCC Rcd 7440, 7443-44 (WTB 1999); *Capitol Radiotelephone*, 11 FCC Rcd at 2335.

[35] Section 301 provides that "[n]o person shall use or operate any apparatus for the transmission of energy or communications or signals by radio . . . except under and in accordance with this chapter and with a license in that behalf granted under the provisions of this chapter." 47 U.S.C. § 301. Section 302(b) provides that "[n]o person shall . . . use devices . . . which fail to comply with regulations promulgated pursuant to this section." 47 U.S.C. § 302(b).

authority under the Communications Act to bypass or waive this prohibition, even when the desired deployment of the technology might be for a legitimate, rather than a malicious, purpose.[36] The only exception recognized by the Commission has been one created by the stature itself, which is for the availability of jamming to *Federal* users under the Commission's jurisdiction.[37] While some have argued that the Commission has the necessary authority to enact regulations which would permit exceptions to the Section 333 restrictions, especially in a prison setting, or that the Section 333 restriction does not apply to interference with "illegal" communications by contraband devices,[38] the Commission has repeatedly and consistently reached the same conclusion with regard to the operation of jammers.[39]

---

[36] The FCC noted in its 1996 decision in *Capitol Radiotelephone* that the legislative history of Section 333 specifically stated that actions "expressly designed to cause interference" include "intentional jamming." *Capitol Radiotelephone*, 11 FCC Rcd at 2335 *citing Section 333 Legislative History, infra*.

[37] A limited exception to the Section 333 prohibition on jamming permits NTIA to authorize jamming by the federal users under its jurisdiction, but the Commission has consistently acknowledged that neither this exception nor any similar exception extends to state entities. *See, e.g.*, *Monty Henry*, 23 FCC Rcd 8293, 8295 (May 27, 2008)(explaining that the Act and Rules exempt "the federal government from the general prohibition" on wireless jammers, but "there is no similar exemption allowing the marketing or sale of unauthorized radio frequency devices to state and local law enforcement agencies"); *Murina C. Ballaro*, 23 FCC Rcd 842, 843 ("While radio frequency devices intended for the federal government or agencies thereof are exempt from the Commission's rules, there is no similar exemption for sales to state and local law enforcement.").

[38] *NTIA NOI*, Comments of Marcus Spectrum Solutions, LLC (Jun. 11, 2010), at 1; *NTIA NOI, Cell Antenna Comments* at 6; *NTIA NOI, GTL Comments* at 4.

[39] The FCC has had a number of opportunities after the *Capitol Radiotelephone* case to consider jamming and its status under the Communications Act. In 1999, the Office of Engineering and Technology and the Compliance and Information Bureau issued a joint Public Notice stating that "the operation of transmitters designed to jam cellular communications is a violation of 47 U.S.C. 301, 302(b), and 333" and that "OET and CIB wish to emphasize that the above regulations apply to all transmitters that are designed to cause interference to, or prevent the operation of, other radio communication systems." Public Notice, *Office of Engineering and Technology and Compliance and Information Bureau Warn Against the Manufacture, Importation, Marketing or Operation of Transmitters Designed to Prevent or Otherwise Interfere with Cellular Radio Communications*, 15 FCC Rcd 6997 (1999). The FCC again addressed the issue in 2005, when in response to multiple inquiries concerning "the sale and use of transmitters designed to prevent, jam or interfere with the operation of cellular and personal communications service (PCS) telephones," the Commission issued a Public Notice to make clear that "the marketing, sale, or operation of this type of equipment is unlawful." Public Notice, *Sale or Use of Transmitters Designed to Prevent, Jam, or Interfere with Cell Phone Communications is Prohibited in the United States*, 20 FCC Rcd 11134 (2005). These authorities were affirmed in FCC denials of requests to conduct the testing and demonstration of jamming equipment in correctional facilities. *See* Letter from Howard Melamed, CEO, CellAntenna Corp., to Marlene H. Dortch, Secretary, Federal Communications Commission (Mar. 3, 2009); Letter from James D. Schlichting, Acting Chief, Wireless Telecommunications Bureau, to Devon Brown, Director, District of Columbia Dept. of Corrections, DA 09-354 (Feb. 18, 2009).

The United States Senate appears to agree with the Commission's interpretation of the Communications Act. In October 2009, the Senate passed the Safe Prisons Act of 2009 which would have amended the Communications Act to authorize the FCC to permit the supervisory authority of a correctional facility to operate a jamming system within the facility to prevent unauthorized wireless communications by individuals held in the facility.[40] Presumably, the Senate would not have felt compelled to act if the Communications Act already permits such action by the Commission. The NTIA concurred in the Commission's analysis in its comparative assessment of managed access with the other interruption technologies.[41]

The Commission has applied a similar Communications Act analysis to managed access, at least as managed access has been designed, deployed and operated at the Parchman, Mississippi prison – *i.e.*, pursuant to spectrum leases obtained from the commercial wireless carriers operating in the prison area – and has reached a very different conclusion.

Under the existing spectrum leasing rules adopted by the Commission,[42] commercial wireless licensees may lease to any qualified third party "any amount of licensed spectrum, in a geographic area or site encompassed by the license, for any period of time during the term of the license."[43] The Commission has specifically permitted leasing arrangements where the licensee and the lessee share use of the same spectrum on a non-exclusive basis."[44] Provided the lease arrangement between the licensee and the lessee satisfies the Commission's approval

---

[40] *Safe Prisons Act, supra.*

[41] *NTIA Report, supra,* at 18 ("The use of jammers by State or local prison officials is a violation of the Communications Act of 1934, and hence illegal.").

[42] 47 C.F.R. §§ 1.9001 *et seq.*

[43] 47 C.F.R. § 1.9003.

[44] Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets, *Second Report and Order, Order on Reconsideration, and Further Notice of Proposed Rulemaking,* 19 FCC Rcd 17503, 17548.

requirements, and such approval is sought and granted, the use of the spectrum within a prison for the simultaneous operation of managed access service for the prison administration does not violate the Commission's rules or Section 333 of the Communications Act.[45] Again, the NTIA has concurred in the Commission's analysis.[46]

*iii. The Pen/Trap Statute – 18 U.S.C. § 3121*

The NTIA identified in its report on interdiction technologies another statute against which wireless interruption technologies must be assessed – the prohibition on pen/trap devices. The so-called "Pen/Trap Statute" states in relevant part that no person may "install or use a pen register or a trap and trace device without first obtaining a court order." A ''pen register'' is a device which records or decodes the "dialing, routing, addressing, and signaling information" transmitted by a device and that such information is "reasonably likely to identify the source of the wire or electronic communication." A "trap and trace device" captures similar information incoming to the device.[47]

The NTIA suggested that, in general, managed access operations may fit the definition of a trap and trace device, and thus might be permitted to operate only pursuant to a court order or under one of the exceptions to the pen/trap statute identified in the law. The NTIA report further suggests, however, that managed access operation might be made to conform with the trap and trace exception which permits the devices to be used when the consent of the user of the

[45] Nor would such operation violates Sections 301 or 302(b) of the Communications Act as the operation of the managed access system in this manner would be pursuant to proper license (and properly licensee lease) and in compliance with the regulations promulgated pursuant to the Communications Act by the Commission. *See* 47 U.S.C. §§ 301, 302(b).

[46] The NTIA has concluded that "[m]anaged access techniques do not violate the Communications Act if the FCC issues the proper authorizations and the users comply with the terms of those authorizations. The NTIA further concluded that "[m]anaged access technology, in hand with proper authorizations from the FCC, may be an effective tool to combat the contraband cell phone problem in correctional facilities" but "to operate a managed access system, the managed access provider requires "a license to transmit and authorization by the carriers servicing the area." *NTIA Report, supra*, at 24-25.

[47] 18 U.S.C. §§ 3121 *et seq*.

communications service has been obtained[48] by establishing a "regime of consent for the usage of a trap and trace device."[49]

The NTIA analysis failed to identify an even more fundamental reason why the operation of a Tecore Managed Access™ system pursuant to FCC and licensee authority, like the Parchman deployment, does not violate the Pen/Trap Statute. Section 3121(b)(1) of the statute specifically exempts wireless service providers from the trap and trace restrictions in the operation and maintenance of their wireless networks.[50] The FCC and licensee authority under which a managed access system like Parchman operates renders the system operator a provider of a telecommunications service and thus exempt from the pen-trap restrictions.

*iv. Sections 201 and 202 of the Communications Act*

Sections 201 and 202 of the Communications Act also must be considered in the analysis of any potential intentional wireless interruption. Any party subject to Section 201 is required to provide communications services "upon reasonable request therefor" and to ensure that its "charges, practices, classifications and regulations for and in connection with such communication service shall be just and reasonable."[51] This is the essence of the communications service provider as a "common carrier." Section 202 goes on to prohibit such common carriers directly or indirectly from making any "unjust or unreasonable discrimination" in its "practices, classifications, regulations, facilities or services … by any means or device" or

[48] 18 U.S.C. § 3121(b)(3).

[49] *NTIA Report, supra,* at 25 n.119.

[50] The section states that the prohibition "does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service relating to the operation, maintenance and testing of a wire or electronic communication service." 18 U.S.C. § 3121(b)(1).

[51] 47 U.S.C. § 201.

subjecting "any particular person, class of persons or locality" to any "undue or unreasonable prejudice or disadvantage."[52]

Section 20.9 of the Commission's Rules defines both cellular and PCS services as common carriers, and in particular as "Commercial Mobile Radio Services" (CMRS), and Section 20.15 specifically makes CMRS licensees subject to Sections 201 and 202 of the Communications Act and other identified Title II requirements.[53] Under this body of law, the question can be asked whether the selective interruption of CMRS wireless services – whether made selective as to time, geography or even class of persons denied service – would violate Sections 201 and 202.

Certainly it has never been mandated that Title II requires common carriers in general, or wireless common carriers in particular, to provide service in ***100%*** of their licensed service areas ***100%*** percent of the time and to ***100%*** of the population. Indeed, such a reading of Title II would be not only without basis in the language of the statute but also without basis in the real world limitations imposed by technology and economics. Sections 201 and 202, by necessity require something less than ubiquitous coverage and ubiquitous service.

Clearly, Title II contemplates limitations in the provision of service by common carriers, and requires only that such limitations be "just" or "reasonable." Acknowledging that service is by nature a limited offering, it has likewise never been mandated *where* and *how* a wireless carrier must provide service within its licensed service areas. While the Commission's Rules provide certain operational and coverage parameters in general terms, it largely has been left up to market forces to determine where a carrier will provide service and to what level of reliability. Thus, the limitation of service based on economic factors is apparently just and reasonable.

[52] 47 U.S.C. § 202.

[53] 47 C.F.R. §§ 20.9(a)(7), (11), 20.15(a).

Similarly, it has never been mandated that a wireless carrier may not engage in scheduled outages for maintenance or other operational or radio engineering purposes, or is operating in violation of law or license if and when portions of its network are rendered inoperable by natural catastrophes, equipment failures, or capacity blocking issues. Clearly, the limitation in service based on technical or operational factors, or due to unforeseen or uncontrollable circumstances, likewise are just and reasonable.

Is it no less just and reasonable to permit the selective interruption of wireless services for certain public safety factors – for example, for the control of contraband wireless devices in prisons and their collateral criminal uses? In a managed access deployment like Parchman, the carriers serving the prison can be seen as having elected to "pull back" their coverage from unauthorized users in a prison in the interest of reducing public risk. Such action is eminently just and reasonable as it targets a geographic area and class of users that are properly to be denied to access their networks because such access is against the law. Is this different that a carrier denying service to someone who might have a legitimate wireless device in their service area but is not a valid subscriber or roamer, or has some payment-related restriction.

*v. Section 20.18 of the Commission's Rules*

Of equal importance in the analysis of any proposed wireless interruption is the mandate to properly handle and complete 911 emergency calls. Section 20.18 of the Commission's Rules requires CMRS providers to "transmit *all* wireless 911 calls without respect to their call validation process." In essence, any incoming 911 call must be completed – even if the call, if it had been a non-emergency call, would not have been completed by the carrier for any reason. The selective interruption of wireless services clearly brings into question whether any resulting

failure by a carrier to complete a 911 call would be deemed to be a violation of Section 20.18 and would subject the carrier to liability.

The answer to the question of CMRS carrier liability for 911 completions in a service interruption scenario may depend upon what role the carrier plays in the service interruption. No carrier has been held liable for failing to complete an emergency call after an involuntary service interruption due to natural disaster or network failure. Likewise, carriers have not been held liable for 911 issues when their network suffers from capacity blocking. Perhaps more importantly, just as there is no mandate on wireless carriers to provide service everywhere and at all times, there is no requirement on wireless carriers to complete 911 calls in those areas within its licensed area where it does not actually offer service. As stated above, the type of service interruption involved with a managed access system in essence amounts to the voluntary action by the carrier community to not provide service to a particular area and class of users. A similar liability analysis should apply as well.

*Authority Exists Under Current Law for the Selective Interruption of Wireless Services*

Section 214 of the Communications Act provides for the interruption of wireless services. Subsection (a) provides for the permanent discontinuance of service, stating that "[n]o carrier shall discontinue, reduce, or impair service to a community, or part of a community, unless and until there shall first have been obtained from the Commission a certificate that neither the present nor future public convenience and necessity will be adversely affected thereby." Subsection (a) further provides for the temporary interruption of service, stating that "the Commission may, upon appropriate request being made, authorize temporary or emergency discontinuance, reduction, or impairment of service, or partial discontinuance, reduction, or impairment of service, without regard to the provisions of this section." An exception is created

in Section 214, however, by the following, which appears to permit any licensee to modify its operations (*i.e.*, "any installation, replacement, or other changes in plant, operation, or equipment, other than new construction") without prior Commission authorization provided that such modifications "will not impair the adequacy or quality of service provided."[54]

Importantly, Section 214 seeks to preserve the "adequacy" of service, and not the universal availability or other similar term. Section 214, then, appears to support the unilateral interruption of service on a temporary basis by any licensee if the interruption does not impair the adequacy of its service. Arguably, the selective interruption of wireless services solely to unauthorized users in prison facilities would not render wireless services in the United States as a whole, or those of any one carrier, inadequate for the public at large. With Commission involvement, however, the requirement for maintaining the adequacy of service would be removed entirely. Seemingly, the Commission is empowered under Section 214 to permit any interruption of wireless services it deems appropriate so long as the public convenience and necessity will not be adversely affected. The selective interruption of wireless service to promote public safety would appear to fall clearly within the realm of actions which would promote, rather than diminish, the public convenience and necessity in light of the careful targeting of such interruptions to corrections facilities.

Section 316 of the Communications Act states that "[a]ny station license or construction permit may be modified by the Commission either for a limited time or for the duration of the term thereof, if in the judgment of the Commission such action will promote the public interest,

[54] 47 U.S.C. § 214(a).

convenience, and necessity." Indeed, when the proposed modification is "where safety of life or property is involved," the Commission may make such modifications on an expedited basis.[55]

It is well settled that the Commission has the authority to modify the terms or imposed conditions on existing licenses if such terms or conditions are reasonably determined to be in the public interest.[56] It is equally well settled that the modification of an outstanding license may occur not only directly through a literal change in its terms, but also indirectly through the grant of other operating authority that may cause interference to the outstanding licensee within its licensed service area.[57] The Commission's authority to modify an existing station license in the public interest is not diminished even when the modification may cause disruption to a licensee's operations.[58] Pursuant to its authority under Section 316, then, the Commission could amend its rules applicable to all commercial wireless licensees to provide for the direct and stable long term access to spectrum for the selective interruption of wireless services in prisons through the operation of managed access systems even when a wireless carrier is reluctant to provide either a solution to the problem themselves or the necessary spectrum rights.

---

[55] 47 U.S.C. § 316.

[56] "No doubt licensees have a strong and legitimate interest in administrative repose … but the Congress gave the Commission the authority in section 316 to override that interest if doing so serves the public interest, convenience and necessity." *Cal. Metro Mobile Communs., Inc. v. FCC*, 365 F.3d 38, 45 (D.C. Cir. 2004) *citing Greater Boston Television Corp. v. FCC*, 149 U.S. App. D.C. 322, 463 F.2d 268, 286-87 (D.C. Cir. 1971) ("administrative finality is subject to certain powers conferred in the FCC by the Act for appropriate cases" such as license modification power conferred by section 316 – *i.e.*, there is "latitude for the FCC to insert conditions protective of the public interest"), *cert. denied sub nom. WHDH, Inc. v. FCC*, 406 U.S. 950, 32 L. Ed. 2d 338, 92 S. Ct. 2042 (1972).

[57] *See, e.g., L. B. Wilson, Inc. v FCC*, 170 F.2d 793 (D.C. Cir. 1948).

[58] *Cal. Metro Mobile Communs., Inc. v. FCC*, 365 F.3d at 46 (arguing that the FCC failed to consider less "draconian" remedies as well as the costs of modification, including lost customers, disruption of service and the station's diminished capacity, the Court of Appeals nevertheless upheld modification of license on finding that action was in the public interest despite even "minor" disruption to licensee operations).

## 2. BASES FOR INTERRUPTING WIRELESS SERVICE

### a. What types of government authorities are most likely to seek intentionally to interrupt wireless service?

*Corrections Administrations Require the Selective Interruption of Wireless Services to Combat Contraband Devices in Prisons*

The scope of these comments is limited to the selective interruption of wireless services in the interest of public safe by and for correctional administrations. Indeed, among corrections officials there is widespread support for a technology solution to the problem of contraband cell phones, and for managed access in particular.

As noted above, a recent survey by the Association of State Corrections Administrators found widespread support for managed access. The comments included:

> [M]anaged cell phone access is the best thing on the market to control cell phones in the correctional setting
>
> [A] managed access system is the best way to prevent inmates from accessing carrier networks using cell phones
>
> Of all of the available technologies that we have reviewed, the most viable option to stop the illegal trafficking and use of cellular telephones by our offender populations is through managed access….All other means of control are either not as effective, do not work as billed, are labor intensive or illegal under the FCC to operate
> It appears to be the best industry option available for mitigating the use of illegal/contraband cell phones in correctional institutions
>
> This is perfect for correctional facility use
>
> The advantages of this system are abundant[59]

[59] *ASCA Survey*, *supra*, at 3, 5.

**b. In what kinds of situations would a government authority potentially seek intentionally to interrupt wireless service? How frequently do these situations arise? For how long would service be interrupted in these situations? How rapidly after the threat to public safety has passed can service be restored?**

*Corrections Administrations Need a Technological Solution to Combat Contraband Devices in Prisons*

As stated above, the scope of these comments is limited to the selective interruption of wireless services in the interest of public safe by and for correctional administrations. In the report on its assessment of technologies to combat contraband phones is prison, the NTIA found that just like the significant growth experienced by the mobile phone industry as a whole since the inception of the analog wireless cell phone network in the early 1980s, the use of cell phones by prison inmates has grown as the U.S. prison population has expanded.

The number of cell phones confiscated by prison officials has dramatically increased in only a few years. In 2006, California correctional officers seized approximately 261 cell phones in the state‘s prisons and camps; by 2008, that number had increased ten-fold to 2,811.[60] Similarly, in 2009, Maryland prison officials confiscated nearly 1,700 phones in 2009, up from approximately 1,200 phones the year before.[61] NTIA did not investigate the causes of increased confiscation of contraband cell phones. The increase in unauthorized cell phone use by inmates and the decreasing ability of traditional detection, search and seizure methods to stem the flow

[60] Special Report, *Inmate Cell Phone Use Endangers Prison and Public Safety*, Office of the Inspector General, State of California (May 2009), http://www.oig.ca.gov/media/reports/BCI/Special_Report_of_Inmate_Cell_Phone_Use.pdf.

[61] State of Maryland Fact Sheet, *Keeping Communities Safe*, Maryland Department of Public Safety and Correctional Services, Feb. 2010.

has caused the mounting concern among correctional administrators across the country that a technology solution is required.[62]

*Service Interruption by Managed Access of Combat Contraband Devices in Prisons Can Be Implemented for as Long as Necessary to Address the Problem, but Can Be Effectively and Immediately Terminated Without Collateral Effect if the Problem Abates*

Managed access solutions can be implemented for as long or as briefly as the problem persists. While there is no indication that the efforts by inmates to obtain and use unauthorized wireless devices within prisons will abate any time in the near future, the solution can grow over time with the development of new wireless technologies to continue to address the problem for as long as necessary. As was pointed out by commenters and the NTIA in the NTIA NOI, any solution to the contraband cell phone problem in prisons needs to address a growing number of telecommunications methods, and Tecore's solution, at least, is designed to be upgradable over time to address, for example, Long Term Evolution (LTE).[63] Yet, in the event the problem of contraband phones is somehow otherwise eliminated, normal wireless services can be restored instantly and without creating collateral issues.

[62] *See* Department of Justice, Office of Justice Programs, National Institute of Justice, *Cell Phones Behind Bars*, (Dec. 2009), http://www.ncjrs.gov/pdffiles1/nij/227539.pdf; Scott McCabe, *Drug Dealer Who Planned Murder Gets Life Sentence*, WASHINGTON EXAMINER (May 4, 2009), http://www.washingtonexaminer.com/local/crime/Drug-dealer-who-planned-murder-gets-life-sentence44327767.html; Vince Beiser, *Prisoners Run Gangs, Plan Escapes, and Even Order Hits With Smuggled Cellphones*, WIRED MAGAZINE (May 22, 2009), http://www.wired.com/politics/law/magazine/17-06/ff_prisonphones. Contraband cell phone use has been noted to be a problem in Federal prison facilities as well. *See* Testimony of Harley J. Lappin, Director, U.S. Bureau of Prisons before the U.S. Congress, Hearing on the Fiscal Year 2009 Budget Request for the Bureau of Prisons, the U.S. Marshal Service, and the Office of the Federal Detention Trustee, http://www.november.org/stayinfo/breaking08/LappinTestimony.html.

[63] [NTIA cite]; *see* AT&T comments at 11.

### c. Under what circumstances would an interruption of wireless service likely be effective in protecting public safety? Under what circumstances might interrupting wireless service be ineffective?

*Tecore's Managed Access™ Solution Has Been Very Successful at Combating Contraband Devices in the Mississippi State Penitentiary*

The effectiveness of Tecore's solution has been proven at its Parchman, Mississippi deployment. As discussed above, in its first 60 days of operation at the Mississippi State Penitentiary, the system blocked over 365,000 call and text message attempts, and has now blocked over 2 million calls and text messages.

*Managed Access Is Effective, However, Only When All Frequencies and Technologies Are Targeted*

To be a successful solution to the problem of contraband wireless devices, a technology must address the *entire* problem. A successful managed access system must insert its authentication and denial capability between *all* contraband devices introduced within the prison and *every* wireless network that makes usable signal available in and thereby enables wireless devices to complete communications. The unavailability of any required spectrum operating right would create a "hole" in the managed access interruption umbrella which would very quickly be exploited by inmates and defeat the entire system.[64]

The NTIA noted in its technology report that managed access "requires structured coordination and cooperation between a managed access system vendor and the wireless service providers in the affected area" and that "[c]oordination of spectrum issues between the FCC, the wireless carriers, and the managed access provider is critical for successful implementation."[65]

[64] Speaking with regard to the introduction of new technologies and frequencies into the commercial wireless environment surrounding a prison, the NTIA observed in its technology report, "It is reasonable to assume that interdiction efforts will not prevent access to a plethora of devices by inmates and that it will not take long for them to find out which devices work and which ones are blocked, dropped, or detected." NTIA Report, at [cite]

[65] *Id.*

Because managed access systems currently can operate only pursuant to a *voluntary* lease of critical spectrum within the limited area of the prison,[66] every wireless carrier serving a prison must agree to provide a spectrum lease before a managed access system can deliver comprehensive interdiction capabilities to prison officials and be worth the cost of installation and operation. No law or regulation currently prevents any wireless carrier from electing *not* to participate and withholding spectrum usage rights for a managed access system. Similarly, Commission Rules do not provide for FCC review of the terms and conditions of a spectrum lease prior to approval. As a result, nothing prevents any wireless carrier from demanding unreasonable lease terms and conditions in exchange for granting spectrum rights for managed access interdiction.

The inevitable by-product of the current regulatory environment already has become evident. Despite the success of the deployment of managed access at Parchman, Mississippi, the expansion of the system to other facilities in that state has been hampered by the refusal of at least one wireless carrier to provide access to its spectrum. Despite the support of CTIA, and the voluntary cooperation of the largest carriers in the United States in the deployment of managed access so far, the recent experience with the Mississippi expansion proves that it is unreasonable to expect all 100+ carriers[67] to voluntarily provide access to their spectrum on reasonable terms.

---

[66] Managed access systems also have operated in the short term pursuant to experimental authorizations from the Commission's Office of Engineering and Technology and Special Temporary Authorities issued by WTB, but both have required prior carrier consents.

[67] In its most recent Mobile Wireless Competition Report, WTB reported that over 100 nationwide, regional and smaller commercial wireless operators currently provide some form of facilities-based cellular or cellular-like service in the United States. Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, including Commercial Mobile Services, WT Docket No. 10-133, *Fifteenth Report*, 26 FCC Rcd 9664, 9693-95 (2011).

## 3. RISKS IN INTERRUPTING WIRELESS SERVICE

### a. What public safety risks arise from intentionally interrupting wireless service? How are the activities of first responders and other emergency personnel and government authorities affected by an intentional interruption of wireless service? How are the activities of consumers affected by an intentional interruption of wireless service?

*The Interruption of Wireless Services Risks the Failure to Complete Emergency Calls Unless the Interruption Technology is Nimble and Can Handle Emergency Calling While Preventing Unauthorized Inmate Usage*

Corrections departments "should have access to technology to disrupt prison cell phone use in a manner that protects nearby public safety and Federal Government spectrum users from harmful disruption of vital services, and preserves the rights of law-abiding citizens to enjoy the benefits of the public airwaves without interference. When considering what interruption technology to implement "it is essential to maintain and protect authorized radio communications (for example, authorized cell phone calls by consumers, *9-1-1 calls* and public safety communication networks), both inside and outside of the prison walls.[68]

In the area of the interruption of wireless devices in prisons, both the National Emergency Number Association ("NENA") and the Association of Public-Safety Communications Officials ("APCO") have expressed their support for non-jamming solutions "because jammers cannot discern between legitimate, illegitimate, 9-1-1 and public safety communications."[69] Five major national wireless carriers – AT&T, C-Spire, Verizon Wireless, Sprint Nextel, and T-Mobile USA – likewise all have supported managed access "due in large

[68] NTIA Report, at 1, 38 [emphasis added].

[69] *Id.* at 21. *See generally* NENA comments; APCO comments. Tecore noted in its comments in the NTIA NOI proceeding that "certain jamming systems can detect the initiation of a 911 call, and can switch off the jamming transmission to allow such a call to connect to the commercial network. However, [d]uring that period, other devices including contraband cell phones may also have access to the commercial network." Tecore comments at Appendix B, n.10. Such operation obviously renders the solution unable to be both effective and responsive to public safety needs.

part to the system's ability to allow public safety, 9-1-1, and authorized calls to reach the cellular networks."[70] The NTIA has observed that with the deployment of the managed access system in Mississippi "the technology was shown to be able to discriminate between authorized calls (including to 9-1-1) and calls from contraband, unknown, and unregistered phones."

*The Interruption of Wireless Services Also Risks The Possibility of Exceeding Its Desired Scope to Affect Communications Not Intended to be Blocked*

In addition to the issue of interrupting emergency calling both inside and outside the target, the wireless interruption also risks unintentionally blocking other authorized communications. It is widely agreed that maintaining and protecting authorized radio communications is essential. As stated above, the NTIA has noted that prison officials deserve access to technology to disrupt prison cell phone use but which also "preserves the rights of law-abiding citizens to enjoy the benefits of the public airwaves without interference."

Berkeley Varitronics Systems ("BVS") has suggested that "[t]he only strategy which may be subject to this concern [*i.e.*, interference with legitimate communications] is jamming.[71] Tecore's Managed Access™ solution, however, has been recognized as having "great potential for addressing the problem...without jeopardizing public safety and commercial communications."[72] Because of managed access has "more precise control over the bands selected for disruption . . . unexpected interference to other services is reduced."[73] Of particular

[70] *Id.*

[71] BVS comments at 5. *See* Illegal Wireless Devices, ANDREW SEYBOLD PERSPECTIVE (Mar. 10, 2009), http://andrewseybold.com/static/public/blog/blog244.html (Mead, Washington school administrators installed jammer to prevent students from using cell phones during school hours and caused interference to Public Safety communications); Torsten Ove, Bars of trouble: Cell Phones in Jail, PHILADELPHIA POST-GAZETTE (Oct. 10, 2008), http://www.post-gazette.com/pg/08284/918854-85.stm (jamming device in Brazilian prison knocks out wireless service to nearly 200,000 nearby residents); Madhuprasad N, Central prison forced to withdraw mobile jammers, DEACON HERALD (May 13, 2006) (jammer in a prison in India disrupts service to people living within five kilometer radius);

[72] AT&T comments at 2.

[73] T-Mobile USA comments at 8.

concern are Nextel/SMR devices, which operate in close proximity to public safety frequencies and use proprietary protocols. Verizon Wireless believes, however, that a managed access system "can intercept Nextel/SMR calls within prisons without interfering with public safety radios.[74] And Sprint Nextel has concluded "that a properly configured managed access system that has been coordinated with the relevant commercial mobile operators would have little likelihood of causing interference to cell phone users outside the prison facility.[75]

**b. What are the potential economic consequences of intentionally interrupting wireless service?**

*The Wireless Industry Has Not Alleged Any Economic Consequence to the Use of Managed Access to Selectively Interrupt Wireless Service in Prisons*

The commercial wireless industry has alleged no economic consequence to the selective interruption of wireless service to corrections facilities. Indeed, CTIA and the four major national carriers all have advocated the deployment of managed access for this purpose. Quite to the contrary, Steve Largent, President and CEO of CTIA, stated in Congressional testimony that CTIA's "carriers have no *legitimate subscribers* residing in these institutions and no interest in seeing inmates use wireless services to conduct unlawful activities or harass or intimidate the public."[76]

[74] Verizon Wireless comments (slides) at 14.

[75] Sprint Nextel comments at 1-2.

[76] Testimony of Steve Largent, President and CEO, CTIA – The Wireless Association® on Contraband Cell Phones in Correctional Facilities: Public Safety Impact and the Potential Implications of Jamming before the Senate Committee on Commerce, Science, and Transportation (Jul. 15, 2009), at 1, http://files.ctia.org/pdf/Testimony_CTIA_Largent_Contraband_Cell_Phones_7_15_09.pdf

**c. How do particular circumstances affect the risks that arise from an interruption of wireless service? Are there particular kinds of locations where interruption is especially risky? Are there areas where first responders and other emergency personnel are especially dependent upon commercial wireless service to perform their duties or where consumers are particularly dependent on wireless service? How does the availability of alternative means of communication affect the risks that arise from an interruption of wireless service? Does the interruption of wireless service pose particular risks to persons with disabilities?**

*Tecore's Solution Has Been Proven at the Rural Parchman Prison and Will Be Further Proven at the Urban Baltimore Metropolitan Transition Center*

As discussed above, the deployment of Tecore's technology at the Mississippi State Penitentiary at Parchman, Mississippi has been enormously successful – not only in terms of the scope of the unauthorized communications stopped by the system, but also in terms of its ability to operate effectively without producing collateral adverse impacts on communications outside the prison grounds.

The Parchman prison is a rural facility that operates as a working farm. The restricted area of the prison campus consists of seven (7) individual prisons disbursed within a four square mile area of the 18,000 acre facility. Figure 1 below shows the rural nature of the Parchman facility.[77] The managed access system at Parchman serves a large area covering all seven of the housing units and a significant portion of the farmland. Figure 2 below shows the area of Figure 1 highlighted in the red square with the nearest major public roadway (US 49 W) highlighted in red as well several miles to the east.

[77] The seven housing units are identified with red squares (and the unit numbers) and the large "X" identifies the location of the main gate onto the secured prison grounds.

***Figure 1***

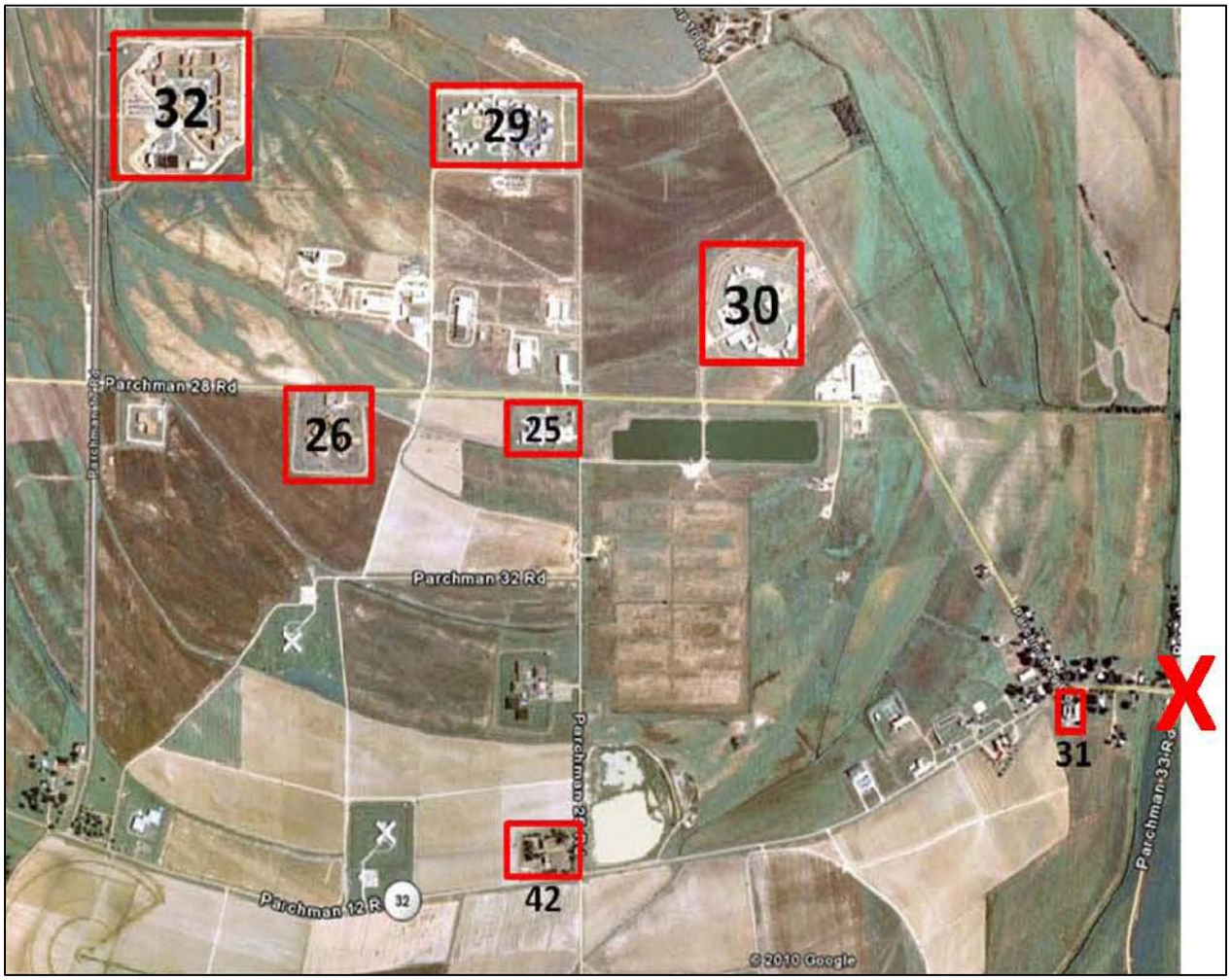
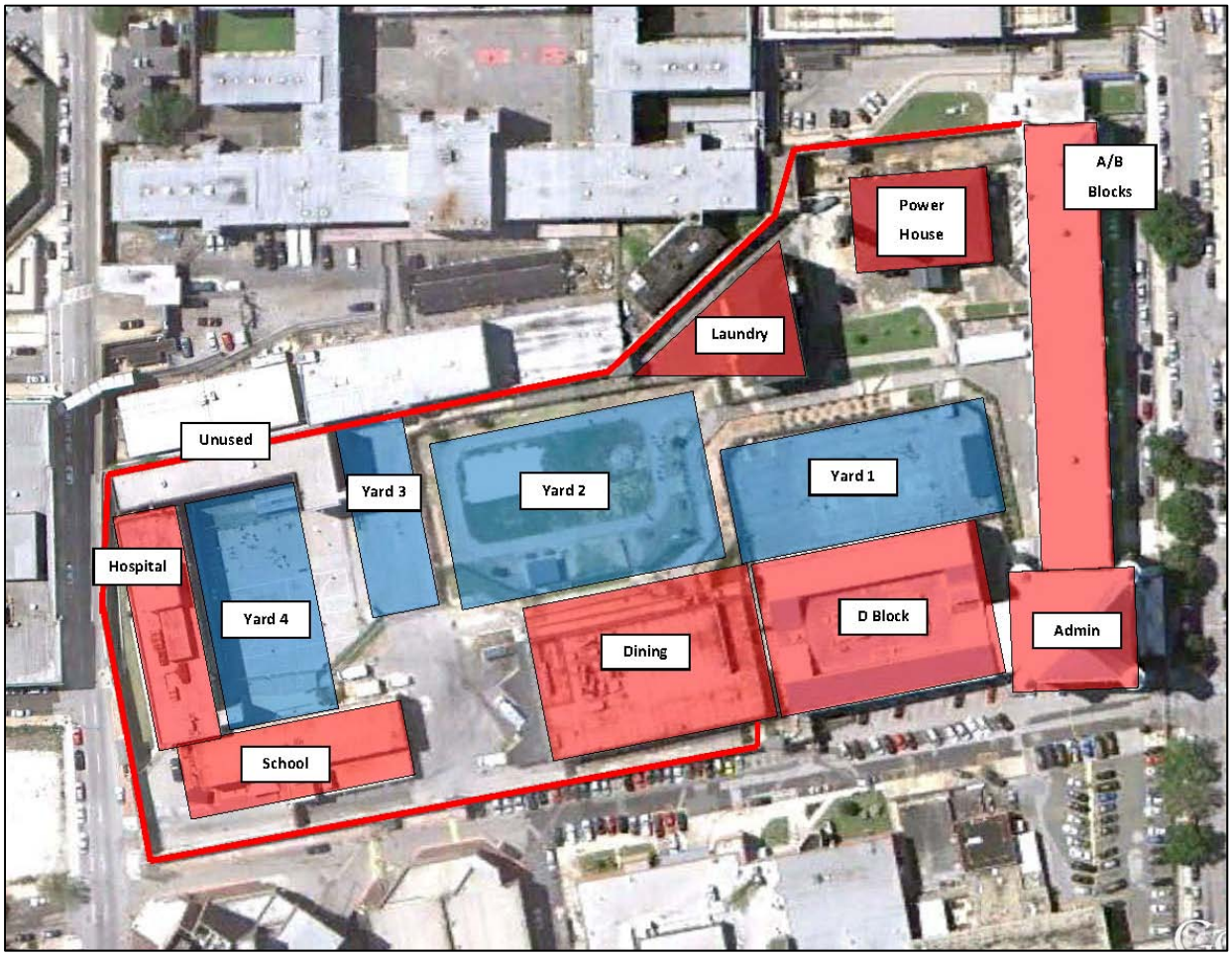

32
29
30
26
25
31
42
X
Parchman 28 Rd
Parchman 32 Rd
Parchman 12 R
Parchman 33 Rd
© 2010 Google

***Figure 2***

A much more challenging environment in which to control unintentional operation of the managed access system outside the restricted areas of the prison will be presented by the upcoming deployment of Tecore's solution at the Metropolitan Transition Center ("MTC") in downtown Baltimore, Maryland. Figure 3 below shows the several buildings and exterior spaces to be covered by the managed access system at the MTC. As the image shows, the MTC campus is an urban one in which the prison facility is directly adjacent to public roadways and buildings.

***Figure 3***




In both the urban and rural environment, and every environment in between, the careful design of the radio frequency transmission equipment is critical. In addition, as the NTIA has observed, "Coordination with commercial service providers ensures that the managed access solution conforms to the boundaries of a correctional facility by matching power output levels. This prevents the system from adversely affecting legitimate radio frequencies outside of the prison, while commanding the spectrum within the prison."[78]

[78] *NTIA Report*, *supra*, at 21.

**d. What steps could be taken to minimize the risks that arise from an interruption of wireless service? What steps could be taken to narrow the scope of a service interruption?**

*The Risks of Interference by Managed Access Systems with Authorized and Emergency Communications Have Been Mitigated*

Various sections above discuss the steps that can be taken to minimize the risks inherent in the interruption of wireless service by managed access, both with regard to the interference with emergency calling and with all communications outside the targeted restriction area, and to narrow the scope of the interruption to the minimum necessary to address the contraband problem.

**e. What institutions or officials should be notified of an intentional interruption of wireless service? How and when should they be notified? How and when should the public be notified? Should notifications include the reason for the service interruption?**

COMMENT NOT OFFERED

**f. Are there less intrusive ways of protecting public safety than interrupting wireless service? If so, what are they? Under what circumstances are these alternative means likely to be as effective as interrupting wireless service? Should government officials be required to consider alternative means before interrupting wireless service?**

COMMENT NOT OFFERED

**g. Are there situations where the risk of interrupting wireless service will always outweigh the benefits?**

COMMENT NOT OFFERED

### h. What kinds of liability issues for wireless service providers might be raised by wireless service interruptions?

*Liability for Wireless Service Providers Resulting From Voluntary or Involuntary Service Interruptions Is Not Supported by the Law*

As discussed above, Sections 201 and 202 of the Communications Act require wireless carriers to provide communications services upon the reasonable request for such services and unjust or unreasonable discrimination, and Section 20.18 of the Commission's Rules requires wireless carriers to transmit all wireless 911 calls. Despite the fact that Section 20.15 of the Commission's Rules specifically makes CMRS licensees subject to Title II requirements, there is no basis for concluding that the selective interruption of wireless services – whether made selective as to time, geography or even class of persons denied service – could result in liability for the wireless carriers.

As further discussed above, it has never been the rule that wireless carriers must provide service to all persons throughout their entire licensed service areas 24/7/365. As noted, such a reading of Title II would be without basis in the statute and without basis in the real world due to the limitations imposed by technology and economics. Wireless service by its nature is a limited offering and wireless carriers have great discretion in determining where and how they will provide service within its licensed service areas. Nor has it ever been mandated that a wireless carrier may not have voluntary or involuntary outages for maintenance or other operational or radio engineering purposes, or is as the result of natural catastrophes, equipment failures or capacity blocking issues. It would appear no less just and reasonable for a carrier to participate – whether voluntarily or involuntarily – in the selective interruption of wireless services for public safety reasons.

Likewise, while the selective interruption of wireless services brings into question the liability which may be associated with a wireless carrier's resulting failure to complete a 911 call, there does not appear to be a firm basis on which to conclude that a wireless carrier should be liable for such a failure, especially when it has not consented to the interruption. No carrier has been held liable for failing to complete an emergency call after an involuntary service interruption due to natural disaster or network failure. Indeed, there is no requirement on wireless carriers to complete 911 calls in any area(s) within its licensed service area in which it does not actually offer service. Should a carrier voluntarily interrupt its wireless service in a prison, or have its service interrupted without its consent, the net result will be a "dead zone" for the carrier, and by definition As stated above, the type of service interruption involved with a managed access system in essence amounts to the voluntary action by the carrier community to not provide service to a particular area and class of users. A similar liability analysis should apply as well.

## 4. SCOPE OF INTERRUPTION

### a. Can wireless carriers implement a general service interruption, but still ensure that the public can make wireless 911 calls? Would a service disruption that permits wireless 911 calls, but otherwise prohibits voice, text, and data communications, achieve the same purpose as a blanket interruption? Would it pose any unique risks to persons with disabilities?

*Wireless Service Interruptions to Address Prison Cell Phones Can and Should Selectively Block Unauthorized Communications but Permit All Emergency Calling Regardless of Source*

In the interest of public safety, and to satisfy the spirit of Section 20.18 of the Commission's Rules, wireless service interruptions for the interdiction of contraband wireless devices within correctional facilities should be implemented only with technologies that are sufficiently nimble to permit the selective blocking of unauthorized communications, yet permit the completion of authorized communications and most importantly all emergency (911)

communications, even if the source is an unauthorized user. Tecore's patened Managed Access solution is such a technology.

The ability to complete all emergency 911 calling not only ensures that even unauthorized callers can report and respond to emergency situations, but also that in the event any authorized caller outside the intended managed access service area in the prison is inadvertently blocked from service, that subscriber nevertheless will not be denied access to critical fire and health care services in the event of an emergency. This not only maximizes the availability of emergency response but also minimizes any potential for liability which might otherwise result from a failed 911 call attempt.

**b. Can wireless carriers implement a service interruption while ensuring that authorized parties would have uninterrupted access to wireless priority service (WPS)?**

COMMENT NOT OFFERED

**c. Can wireless carriers implement a service interruption and still provide targeted alerts via the Personal Localized Alerting Network (PLAN) to the public in the affected area?**

COMMENT NOT OFFERED

**d. What are the costs and benefits of a service interruption where one or more of wireless 911, WPS, or PLAN are also disrupted?**

COMMENT NOT OFFERED

**e. What are the different methods for interrupting wireless service? How do circumstances affect the availability of these methods?**

COMMENT NOT OFFERED (the NTIA Report provides information on jamming as an alternative method of service interruption)

**f. How do the effects differ among methods of interruption? Do some methods target a narrower geographic area?**

COMMENT NOT OFFERED (the NTIA Report provides information on jamming as an alternative method of service interruption)

**g. What methods of interrupting service would lead to the most rapid restoration of service?**

COMMENT NOT OFFERED (the NTIA Report provides information on jamming as an alternative method of service interruption)

## 5. AUTHORITY TO INTERRUPT SERVICE

**a. What processes could ensure that only an appropriate official makes the decision to request an interruption of wireless service? How would such an official be contacted in an emergency situation where time is of the essence?**

COMMENT NOT OFFERED

**b. What institutions or officials should be able to review the decision to interrupt wireless service? What process considerations or safeguards should be implemented? How can timeliness of such review be ensured?**

COMMENT NOT OFFERED

**c. What obligations do or should wireless carriers have to comply with a request by a government official to interrupt wireless service?**

*Commercial Wireless Carriers Are Not Currently Required to Participate in Wireless Service Interruption as a Means to Combat Contraband Prison Cell Phones*

As discussed above, managed access systems currently can operate only pursuant to a voluntary lease of spectrum by commercial wireless providers operating in the area of the prison. *Every* wireless carrier serving a prison must agree to provide spectrum lease before a managed access system can deliver comprehensive interdiction capabilities to prison officials and be worth the cost of installation and operation. No law or regulation currently prevents any wireless carrier from electing to withhold spectrum usage rights for a managed access system. Similarly, Commission Rules do not provide for FCC review of the terms and conditions of a spectrum lease prior to approval. As a result, nothing prevents a wireless carrier from demanding unreasonable lease terms and conditions in exchange for granting spectrum rights for managed access interdiction.

The inadequacy of this current regulatory environment already has become evident. Despite the success of the deployment of managed access at the Parchman facility in Mississippi, the expansion of the system to other facilities in that state has been hampered by the refusal of certain wireless carriers to provide access to spectrum.

The problem will likely only get worse. With over 100 commercial wireless operators currently providing some form of facilities-based wireless service in the United States, the experience with the Mississippi expansion proves that it is unreasonable to expect that all 100+ carriers will voluntarily provide access to their spectrum on reasonable terms in order for managed access to be deployed successfully in every locale where local corrections officials deem the solution vital to addressing their losing battle with contraband communications.

**d. What steps should be taken to ensure a timely return to full wireless service in the affected area? What institutions or officials should have authority to request a return to full wireless service in the affected area?**

*The Authority to Operate a System to Selectively Interrupt Wireless Services Should Cease When the Operation of the System is No Longer Needed To Address the Public Safety Concern At Issue*

Currently, as previously discussed, the operation of managed access as a wireless interruption technology to address the public safety issue caused by the rampant availability of contraband wireless devices in our prisons currently may be carried out as a result of the cooperation of commercial wireless carriers in granting voluntary access to their spectrum through FCC-approved spectrum leases. Such lease agreements can and should be self-regulating and thereby provide for the termination of the lease and the spectrum rights therein when it is determined by the corrections administration being served that the service interruption is no longer needed or effectively addresses the problem.

In the event the Commission takes steps to amend its Rules to provide for the granting of direct authority for corrections officials to operate wireless interruptions systems in their prisons

whenever the necessary wireless carriers are unwilling to provide their own solution or grant access to their spectrum, the direct authority should be similarly limited in scope such that the authority will lapse whenever it is determined by the corrections administration licensee that the service interruption is no longer needed or effectively addressing the contraband problem.

**e. What procedures should there be to review an interruption after it has occurred?**

COMMENT NOT OFFERED (see previous section)

## 6. LEGAL CONSTRAINTS ON INTERRUPTING WIRELESS SERVICE

**a. What sources of legal authority does the Commission have regarding shutdowns of wireless service? What discretion does the Commission have to approve or disapprove shutdowns?**

*The Commission Has The Authority to Grant Direct Authority to Prison Officials to Operate a Managed Access System in the Event Wireless Carriers Volunteer Spectrum Rights*

Given the national public safety implications resulting from the increasing availability of unauthorized wireless communications to inmates, and the growing list of illegal activities that have been perpetrated by inmates with the aid of unauthorized devices, it is unacceptable that any carrier licensed by the Commission to operate on the public airwaves can be permitted to stand in the way of the deployment of a proven technological solution to the problem, and that corrections officials are to be left with no means to employ effective, legal technology available today if the voluntary and reasonable cooperation of carriers is not forthcoming. Clearly, in light of the paramount importance to public safety and the administration of justice represented by the effective control of illegal communications by inmates, creating a means by which managed access systems can be deployed even in the absence of voluntary cooperation by commercial wireless carriers is squarely in the public interest. Given the significant cost of installing and operating a technology solution like managed access, it is difficult for prison systems to justify

the expenditure if they are not assured of the necessary access to the spectrum needed to operate the system for the long term.

As discussed above, Section 316 of the Communications Act gives the Commission the authority to modify the terms of wireless licenses during the term of such licenses "if in the judgment of the Commission such action will promote the public interest, convenience, and necessity." In fact, where the proposed modification is one "where safety of life or property is involved," the Commission may modify a license on an expedited basis.[79] It is well settled that the Commission has the authority to modify the terms or imposed conditions on existing licenses if such terms or conditions are reasonably determined to be in the public interest.[80] It is equally well settled that the modification of an outstanding license may occur not only directly through a literal change in its terms, but also indirectly through the grant of other operating authority that may cause interference to the outstanding licensee within its licensed service area.[81] The Commission's authority to modify an existing station license in the public interest is not diminished even when the modification may cause disruption to a licensee's operations.[82]

---

[79] 47 U.S.C. 316(a)(1).

[80] "No doubt licensees have a strong and legitimate interest in administrative repose … but the Congress gave the Commission the authority in section 316 to override that interest if doing so serves the public interest, convenience and necessity." *Cal. Metro Mobile Communs., Inc. v. FCC*, 365 F.3d 38, 45 (D.C. Cir. 2004) *citing Greater Boston Television Corp. v. FCC*, 149 U.S. App. D.C. 322, 463 F.2d 268, 286-87 (D.C. Cir. 1971) ("administrative finality is subject to certain powers conferred in the FCC by the Act for appropriate cases" such as license modification power conferred by section 316 – *i.e.*, there is "latitude for the FCC to insert conditions protective of the public interest"), *cert. denied sub nom. WHDH, Inc. v. FCC*, 406 U.S. 950, 32 L. Ed. 2d 338, 92 S. Ct. 2042 (1972).

[81] *See, e.g., L. B. Wilson, Inc. v FCC*, 170 F.2d 793 (D.C. Cir. 1948).

[82] *Cal. Metro Mobile Communs., Inc. v. FCC*, 365 F.3d at 46 (arguing that the FCC failed to consider less "draconian" remedies as well as the costs of modification, including lost customers, disruption of service and the station's diminished capacity, the Court of Appeals nevertheless upheld modification of license on finding that action was in the public interest despite even "minor" disruption to licensee operations).

To resolve the roadblock currently presented to corrections officials around the country by wireless carriers who choose not to voluntarily provide access to their spectrum on reasonable terms and conditions, and to assure these corrections departments that they can procure and operate the tools they need to combat contraband devices and the illegal activity they facilitate, the Commission should immediately initiate a rulemaking proceeding to amend its rules applicable to all commercial wireless licensees around the country to provide for the following:

*In the event that any Federal, state or local corrections agency (or its designated agent or representative) states in writing to any licensee that:*

*(a) the use of wireless devices is prohibited or restricted by applicable law, regulation or policy within one or more of its secured corrections facilities;*

*(b) the agency desires to implement a managed access wireless interdiction system within such facility(ies), and*

*(c) such facility(ies) are located within the licensed geographic service area of the licensee,*

*then within 90 days thereafter, either:*

*(x) the licensee shall:*

*(1) restrict the access of unauthorized wireless devices to its service within the interdiction zone(s) identified by the agency either by:*

*(i) modifying its operations under the affected license(s), or*

*(ii) installing and operating its own system to manage access within the interdiction zone(s) to its service provided under the license, or*

*(2) execute a long term spectrum lease with the agency (or its designated agent or representative) on fair and reasonable terms for the duration of its license(s) pursuant to which the agency (or its designated agent or representative) shall have the right to operate a managed access system within the identified interdiction zone(s) without causing harmful interference to the operations of the licensee outside the interdiction zone(s), or*

*(y) the agency may:*

*(1) request a Private Mobile Radio Service license to install and operate the managed access system (either directly or through its agent or representative), and*

*(2) such license shall be granted within 30 days thereafter if the Commission determines that the grant of such license is in the public interest.*

**b. Are there circumstances under which a government entity could be construed to have common carrier obligations under the Communications Act due to its relationship with or control over wireless service?**

*The Operator of a System for Wireless Service Interruption May Be Deemed To Be a Common Carrier Unless Formal Steps Are Taken to Achieve a Different Classification*

A government entity or its designated representative deploying and operating a system to selectively interrupt wireless service, like a managed access system, which operates under lease authority from a CMRS licensee or within its own direct authority from the Commission might

be deemed to have common carrier obligations unless steps are taken to operate the system so that it may be classified as something other than a common carrier/CMRS service, and as such fall outside the requirement to satisfy Title II and other common carrier service obligations. For example, the service may operate as a Private Mobile Radio Service, and seek a formal declaration of such status from the Commission.

**c. What authority does the Commission have to preempt laws and regulations permitting or prohibiting interruption of wireless service? How should the Commission exercise any such authority?**

*The Proposed Rules Do Not Require the Commission to Preempt Any Law Prohibiting the Interruption of Wireless Service*

The proposed rules set out in the previous section may be implemented by the Commission consistent with its current authority under the Communications Act and its own Rules. The requested action requires no preemption of any law prohibiting the interruption of wireless services.

**d. What protections do the First Amendment or due process rights provide for users of wireless service? Under what circumstances could an interruption of wireless service violate the First Amendment or due process rights of wireless users? Are there other constitutional protections that should be considered?**

COMMENT NOT OFFERED

**e. What protections do the First Amendment, due process, or other constitutional rights afford wireless carriers? Under what circumstances could a forced interruption of wireless service violate the First Amendment, due process, or other constitutional rights of wireless carriers?**

COMMENT NOT OFFERED

**f. What provisions of Title II of the Communications Act prohibit or circumscribe an interruption of wireless service, and under what circumstances? To what extent do sections 202, 214, 302a, 333, or other sections of the Communications Act circumscribe the ability of government actors to interrupt wireless service?**

COMMENT NOT OFFERED (see previous discussion above)

**g. What state laws prohibit or circumscribe an interruption of wireless service? What authorities do state public utility commissions have to prohibit or circumscribe an interruption of wireless service? Are there circumstances in which approval of a state public utilities commission is necessary before ordering a shutdown?**

COMMENT NOT OFFERED

**h. To what extent does a public agency's contractual or practical control over wireless service equipment affect the analysis of whether a public agency has the legal authority to interrupt wireless service?**

COMMENT NOT OFFERED

**i. What is the scope of the Commission's discretion to set policies that affect a public agency's legal authority to interrupt wireless service? To the extent the Commission has not exercised this discretion, should it do so, and in what ways?**

COMMENT NOT OFFERED

**CONCLUSION**

As discussed in these comments, to be a comprehensive solution to the problem of contraband devices, a managed access system must insert its authentication and denial capability between *all* contraband devices and *every* wireless network that can serve them within the prison grounds. The system must operate within all of the radio frequency bands on which all commercial carriers providing a usable wireless signal to the prison are operating. Under current Commission rules, managed access systems must operate as a lessee of spectrum from the commercial wireless licensees in the prison area. The participation of the commercial wireless operators is voluntary, and prison officials must obtain the cooperation of all wireless carriers in order to operate a comprehensive managed access solution. Any carrier that does not provide spectrum rights leaves a hole in the interdiction umbrella which will be exploited by inmates.

No regulation currently prevents a wireless carrier from opting not to permit interdiction within its spectrum or from making spectrum available only under terms and conditions that are

unreasonable, unworkable or which undermine the economic feasibility of managed access. The inadequacy of this regulatory environment already is evident.

While there has been excellent cooperation from the commercial wireless industry as a whole during the development and of managed access by Tecore -- five major commercial wireless carriers (AT&T, C-Spire, Sprint Nextel, T-Mobile and Verizon) each have supported the deployment of managed access systems and have volunteered spectrum rights for the testing and deployment of these systems and the CTIA has endorsed managed access as its preferred technology solution for the interdiction of contraband devices – it is unacceptable that any carrier licensed by the Commission to operate on the public airwaves can block the deployment of a proven technological solution to the contraband problem and leave corrections officials with no means to employ an effective technology solution.

In light of the paramount importance to public safety and the administration of justice represented by the effective control of illegal communications by inmates, it is squarely in the public interest for the Commission to create a means by which managed access systems may be deployed even in the absence of wireless carrier cooperation. Given the significant cost of installing and operating a technology solution like managed access, it is difficult for prison systems to justify such expenditures if they are not assured of stable, long term access to spectrum.

Respectfully submitted,

**TECORE NETWORKS**

By Stephen D. Hayes
Its Vice President and General Counsel