Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
Preventing Contraband Cell Phone Use in Prisons	)	Docket No. 100504212-0212-01
	)	
	)	
	)	

COMMENTS OF T-MOBILE USA, INC.

Kathleen O'Brien Ham
Eric Hagerson
T-Mobile USA, Inc.
401 9th Street
Suite 550
Washington, DC 20004

June 11, 2010

TABLE OF CONTENTS

Page

Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
Preventing Contraband Cell Phone Use in Prisons	)	Docket No. 100504212-0212-01
	)	
	)	
	)	

COMMENTS OF T-MOBILE USA, INC.

T-Mobile USA, Inc. hereby submits the following comments in response to the National Telecommunications and Information Administration ("NTIA") Notice of Inquiry ("NOI") on Preventing Contraband Cell Phone Use in Prisons.[1] T-Mobile appreciates the serious problem posed by contraband cell phone use in prisons. However, wireless jamming, which would be both dangerous and ineffective, is an inappropriate approach to addressing this problem in light of the existence of far superior alternatives. In continuing to investigate this challenge, NTIA should focus on technologies such as managed access and cell phone detection, which not only offer the capability to disrupt illicit cell phone use without the risk of interference with authorized or public safety communications, but also have the potential to gather intelligence helpful in law enforcement operations, such as preventing contraband from entering prison facilities.

I. WIRELESS JAMMERS CAUSE MORE PROBLEMS THAN THEY RESOLVE.

In the *NOI*, NTIA seeks comment on three broad categories of potential solutions for preventing illegal cell phone use in federal prisons: wireless jammers, managed

[1] NTIA, Preventing Contraband Cell Phone Use In Prisons, *Notice of Inquiry*, Docket No. 100504212-0212-01, 75 Fed. Reg. 26733 (2010) ("*NOI*").

access systems and cell phone detection.[2] As discussed herein, wireless jamming is a suboptimal solution for this problem, because it is simultaneously over-inclusive, in that jamming is likely to disrupt a significant amount of legitimate communications, and under-inclusive, because jamming technology will have difficulty keeping pace with the dynamic nature of the wireless industry. In light of the significant drawbacks of wireless jammers, NTIA should not recommend their use in the federal prison system.

Radio jamming has been used strategically to block or interfere with unwanted transmissions for at least the last 70 years, and the premise behind the technology has remained relatively static throughout that time. A jammer works by sending out transmissions on the same frequencies as those used for wireless communications. The jamming signal must be strong enough to overpower the desired signal, thereby disrupting the link between the phone and the base station and rendering the wireless device inoperable. By the nature of the technology, jammers do not discriminate between different users or types of calls—all cell phone communications within range of the jammer and on the frequencies being jammed will be disrupted.

A. Wireless Jammers Are Likely To Significantly Disrupt Public Safety and Other Legitimate Communications.

Wireless jammers represent a serious risk to health and safety because their use has the potential to block communications to, from, and between public safety and first responders. Major groups representing the public safety community, such as the Association of Public-Safety Communications Officers ("APCO") and the National Emergency Number Association ("NENA"), have voiced concern about the use of wireless jamming equipment in federal prisons because of the danger it poses to

[2] *See NOI*, 75 Fed. Reg. at 26735-36.

legitimate communications.[3] Because jammer deployments in federal prisons would likely result in interference to critical public safety communications, both inside and outside the facilities in question, use of these devices should not be permitted.

The most serious problem with wireless jammers, and one which should in itself settle the issue, is that they block all wireless calls made within their range, including calls to 9-1-1. The ability to successfully place a 9-1-1 call is such an essential requirement that Federal Communications Commission ("FCC") rules stipulate that even emergency calls placed from deactivated cell phones must be routed to a Public Safety Answering Point.[4] Authorized cell phone users, such as prison employees, may find themselves unable to call for help in times of emergencies. And, there is a strong possibility, as discussed below, that this technology will disrupt some legitimate emergency communications made from outside the prison facility.

In addition to 9-1-1 calls, it is highly likely that wireless jammers will further disrupt critical communications through interference with pubic safety land mobile radio ("LMR") communication systems. Many of these LMR systems operate in the 800 MHz band, which is directly adjacent to the primary 850 MHz cellular band, and in the nearby public safety narrowband communications allocation in the upper 700 MHz band. As such, one possible unintended and unacceptable consequence of these devices may be substantial disruption to critical communications by public safety and first responders

---

[3] *See* Letter from Chris Fischer, President, APCO to Michael Copps, Acting Chairman, Federal Communications Commission, WT Docket No. 09-30 (filed Mar. 13, 2009); Letter from Brian Fontes, Chief Executive Office, NENA to Michael Copps, Acting Chairman, Federal Communications Commission, WT Docket No. 09-30 (filed Mar. 17, 2009).

[4] *See* 47 C.F.R. § 20.18(b) ("CMRS providers subject to this section must transmit all wireless 911 calls without respect to their call validation process to a Public Safety Answering Point").

called into the prison during times of emergency. For example, a prison may discover at the worst possible time that that its wireless jammers disrupt the mobile communications systems of the local fire department. This problem will be further exacerbated upon deployment of next generation wireless networks in the 700 MHz public safety broadband spectrum, which is directly adjacent to several commercial 700 MHz blocks.

Beyond emergency communications, wireless jammers within prisons are an undesirable solution to the problem of illicit cell phone use because they will disrupt legitimate non-public safety calls. As mentioned above, jammers are a blunt instrument and have no means of distinguishing between authorized and unauthorized cell phone use. Consequently, even perfectly acceptable cell phone calls, such as those placed or received by prison employees on wireless devices, will be blocked.

Compounding this problem is that jammer signals are difficult to confine within the perimeter of a prison complex. These devices operate on commercial mobile radio service ("CMRS") frequencies, which are allocated, in part, based upon their ability to penetrate walls and propagate usefully over a large area on limited power. Furthermore, for any jamming system to be effective, it is imperative that it cover the entire prison complex. However, prisons are designed, quite appropriately, according to a different set of priorities and principles rather than on the proper containment of radio signals. Although jammer vendors may assert that through the use of directional antennas and other techniques they can limit the coverage of the jammer signal, the reality is that to properly cover an entire prison, it is almost impossible to prevent the jammer from affecting communications outside the perimeter of the prison as well.

The possibility for "over jamming" was, in fact, demonstrated in NTIA's recent study on wireless jammer emissions. In that study, even in areas outside the test facility "where jamming was not intended, the results showed that jammer power was measurable at distances up to 127 m from the building."[5] Especially in the urban context, this over jamming will inevitably disrupt legitimate wireless use by individuals near to, but outside of, a prison complex. This likelihood significantly exacerbates the problem of 9-1-1 blocking, discussed above, as private individuals with no expectation of service disruption might be unable to summon emergency services as necessary outside of the prison. Worse yet, this jamming would come with no concomitant public interest benefit.

The problems of over jamming identified above are far from theoretical. Indeed, these problems have been observed on multiple occasions when jammers have been deployed by well-intentioned institutions in the U.S. For example, in 2009, a high school in Spokane, WA, experimented with a cell phone jammer as a means to prevent phone calls and text messaging by students during class periods.[6] Unfortunately, the device also disrupted the cross-band repeater placed in the school by the county sheriff in order to facilitate communications between local police and SWAT responders during times of emergency.[7] Similarly, interference with legitimate commercial communications

---

[5] Frank H. Sanders & Robert T. Johnk, Dept. of Commerce, NTIA, *Emission Measurments of a Cellular and PCS Jammer at a Prison Facility* at xi, NTIA Report TR-10-466 (May 2010).

[6] *See* "School Invests In Cell Phone Jammer to Block Teenage Texting," KHQ.com, Mar. 6, 2009 *available at* http://www.khq.com/global/story.asp?S=9963126 (last visited June 8, 2010).

[7] *See* Andrew M. Seybold, Wireless Jamming Devices Are Illegal and Dangerous, FierceWireless.com, Mar. 10, 2009 *available at* http://www.fiercewireless.com/story/wireless-jamming-devices-are-illegal-and-dangerous/2009-03-10 (last visited June 8, 2010).

occurred when an illegal jammer was deployed by the Agate School District in Colorado.[8] Moreover, as CTIA has documented, cell jammers previously installed in prisons have caused significant unintended disruptions to authorized communications, including blocking cell phone service to 200,000 people in Brazil and jamming cell phone operations over a five kilometer radius in Bangalore.[9] Due to the potentially devastating effects that jammers can have on legitimate communications, their use in prisons should not be allowed.

B. Wireless Jammers May Not Sufficiently Block All Illicit Cell Phone Use Within Prisons.

In addition to the problem of over jamming, there is a very real risk that wireless jammers installed in prisons will not sufficiently block all illicit communications. The wireless industry is extremely dynamic; new technologies and new frequency bands are continually being introduced into marketplace. For each such innovation, a new wireless jammer may be required. Prisoners are notoriously resourceful and will be quick to exploit any weaknesses in the jammer system and to identify unjammed bands. To properly block all possible mobile communications bands, in addition to the 850 MHz cellular, 1900 MHz PCS, and 2100 AWS bands currently used for CMRS services, jamming is also required to cover the 800 MHz public safety, 900 MHz iDEN, 700 MHz LTE, and the various mobile satellite service allocations. A byproduct of this challenge is that each time a new jammer band is added, the possibility of additional interference to

---

[8] *See* Steve Largent, President and CEO, CTIA—The Wireless Association, Testimony Before the Senate Committee on Commerce, Science, and Transportation, July 15, 2009 *available at* http://files.ctia.org/pdf/Testimony_CTIA_Largent_Contraband_Cell_Phones_7_15_09.pdf (last visited June 8, 2010).

[9] *See* Petition to Deny of CTIA—The Wireless Association, Federal Communications Commission WT Docket No. 09-30 at 7-8 (filed Mar. 13, 2009)

unrelated third parties—even on other frequencies, through, for example, intermodulation—increases significantly.

Finally, the constantly changing pattern of wireless network deployment will also negatively impact the effectiveness of jammer solutions. As discussed above, jammers operate by transmitting a jamming signal that is received at the mobile device at a greater power than the signal being sent out by the actual base station. However, wireless providers are constantly improving and adjusting their network coverage in order to maximize service area and quality. If additional commercial network infrastructure is deployed in the vicinity of a prison, it may increase the received power from the base station sufficiently to nullify the effect of the jammer. Thus, jammers not only are likely to block significantly more communications than are desired, these devices also have the potential to do so while failing to serve their intended purpose.

II. MANAGED ACCESS AND CELL PHONE DETECTION ARE BETTER TECHNOLOGICAL SOLUTIONS

Wireless jammers are a particularly undesirable solution to the problem of contraband cell phone use in prisons in light of the existence of superior technological alternatives, which provide additional flexibility for correctional authorities and avoid many of the problems of wireless jammers discussed above. In particular, managed access and cell phone detection systems provide means for prison officials to identify and apprehend users of illicit cell phones without causing disruption to 9-1-1 calls, public safety communications, or other legitimate uses of wireless technologies. Both alternatives also offer additional intelligence gathering and crime prevention capabilities that are not replicated by wireless jammers.

A. Managed Access Systems Provide Maximum Flexibility to Correctional Authorities Without Many of the Pitfalls of Wireless Jammers.

Managed 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. A managed access system is essentially a specialized microcell that intercepts any wireless call made in the prison and compares the information about the device placing the call with a predefined list to determine whether the call should be allowed.[10] Calls that are identified as authorized are allowed to proceed to the applicable commercial network, while illegitimate calls are captured by the managed access system and prevented from being completed.

Managed access systems provide enhanced control for prison officials in terms of distinguishing between legitimate and illegitimate calls. As an initial matter, such systems can be configured to allow all 9-1-1 calls, regardless of the originating device. They also provide more precise control over the bands selected for disruption, thus preventing interference with public safety wireless communications bands. Moreover, managed access systems can employ GPS, directional antennas, and software-based solutions to substantially reduce or even eliminate their effect on communications occurring outside of the prison.

Unlike the all-or-nothing approach of wireless jammers, managed access also provides significant operational flexibility to correctional officers, increasing their

---

[10] *See, generally*, Tecore Networks, White Paper: Intelligent Network Access, Precision Control of Communications in Secured Areas (Nov. 2008) *available at* http://www.tecore.com/solutions/whitepaper.cfm (free registration required).

usefulness in intelligence gathering and crime prevention. Consistent with local wiretap and surveillance laws, managed access systems may allow prison officials to observe who is using illicit cell phones in prisons, identify whom they are contacting or being contacted by, and perhaps even monitor the content of the communications. These capabilities can provide crucial information to law enforcement officials about criminal activity occurring within and outside of the prison, can assist in disrupting smuggling, and can help identify corrupt prison workers.

While managed access solutions, like cell jamming, are band specific, this weakness is shared by all of the technological solutions being considered. Unlike wireless jammers, however, managed access systems use nearly identical emissions to commercial mobile radio base stations and thus, the potential for unexpected interference to other services is reduced.

B. Cell Phone Detection Also Avoids Many of the Problems of Wireless Jammers While Still Addressing the Problem of Contraband Cell Phones.

Cell phone detection solutions, which rely upon a system of sensors placed around a prison facility that identify when a cell phone is being used,[11] are preferable to jamming because they can allow prison officials to locate, monitor over time, and intervene with users of contraband cell phones, but they do not interfere with crucial public safety or other legitimate communications. Cell phone detection systems vary in

[11] *See* ITT Corporation, Detecting and Locating Cell Phones in Correctional Facilities at 3 (June 11, 2007) *available at* http://iiw.itt.com/files/CellHound_wpCellPhonesInPrison.pdf.

their functionalities and sophistication, but generally these systems provide information about the location of an active cell phone and may provide additional data about its use.[12]

Although not providing a technological means of disrupting cell phone communications, cell phone detection systems can assist correctional officers by identifying with a high degree of accuracy the locations where cell phones are being used and stored. This information can be used for subsequent searches and interventions, or as intelligence gathering for larger operations intended to identify the sources and pattern of smuggled goods in prisons. Moreover, cell phone detection systems provide one viable means of addressing the problem of contraband cell phones in prison that poses no threat of interference with 9-1-1, public safety communications, or other legitimate cell phone use.

III. FEDERAL LAW AND POLICY COMPELS THE DEPARTMENT OF COMMERCE TO GIVE MORE COMPLETE CONSIDERATION TO ALTERNATIVES TO JAMMING

Beyond the public safety and practical concerns discussed above, interference-causing jamming technologies currently are prohibited by federal law. In particular, Section 333 of the Communications Act 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 this chapter or operated by the United States Government."[13] The provision has been consistently relied upon by the FCC in

---

12 *See* Maryland Dept. of Public Safety and Correctional Services, Overview of Cell Phone Demonstration at 5 (2009) *available* at http://www.dpscs.state.md.us/publicinfo/media/pdf/FinalReport_2008-09-10.pdf (providing information about a demonstration of various cellular detection systems).

13 47 U.S.C. § 333.

enforcement actions against marketers and users of wireless jammers,[14] and the FCC has made clear that the "marketing, sale, or operation of this type of equipment is unlawful."[15] Indeed, the FCC has also denied multiple requests to test jamming equipment in prisons because of the clear prohibition on their operation.[16]

The Communications Act does not prevent the federal government from using wireless jamming equipment; however, it does establish a strong policy position that disfavors the use of such devices. Allowing the use of jammers in federal facilities would create confusion because it would still be illegal to use such devices in non-federal institutions. Furthermore, allowing jammers could result in an increase in the availability of jammers on the open market, which would doubtlessly lead to more unauthorized use of these devices.

The federal policy opposed to jammers is further evidenced by the fact that NTIA was specifically instructed by Congress to consider non-jammer technologies as a response to the problem of contraband cell phone use in prisons. As the *NOI* indicates,[17] the current proceeding was prompted by language in the Conference Report to the

---

[14] *See, e.g.*, Federal Communications Commission, Citation, *DPL Surveillance Equipment*, DA 08-1202, 23 FCC Rcd 8293 (2008); Federal Communications Commission, Citation, *Phonejammer.com*, DA 08-1193, 23 FCC Rcd 8264 (2008).

[15] Federal Communications Commission, Public Notice, *Sale or Use of Transmitters Designed to Prevent, Jam or Interfere with Cell Phone Communications is Prohibited in the United Sates*, DA 05-1776, 20 FCC Rcd 11134 (2005).

[16] *See, e.g.*, Letter from James D. Schlichting, Acting Chief, Wireless Telecommunications Bureau, Federal Communications Commission to Devon Brown, Director, District of Columbia Department of Corrections, DA 09-354, 24 FCC Rcd 2060 (2009); Letter from James D. Schlichting, Acting Chief, Wireless Telecommunications Bureau, Federal Communications Commission to Howard Melamed, Chief Executive Officer, CellAntenna Corporation, DA 09-622, 24 FCC Rcd 3246 (2009).

[17] 75 Fed. Reg. at 26734.

Department of Commerce FY 2010 Appropriations, which tasked NTIA with developing a plan to "investigate and evaluate how wireless jamming, detection and other technologies might be utilized for law enforcement and corrections applications in Federal and State prison facilities."[18] This same provision urged NTIA "to investigate and evaluate detection or other technologies that do not pose a risk of negatively affecting commercial wireless and public safety services in areas surrounding prisons."[19]

As discussed above, managed access and cell phone detection systems do not pose the same risks of harmful interference that are associated with wireless jamming. Although NTIA has undertaken detailed technical studies on jamming technology,[20] no similar studies have been conducted on managed access or cell phone detection technologies, which are among the sorts of alternatives Congress strongly urged NTIA to consider. Moreover, because of their enhanced intelligence-gathering potential, which could be of great assistance in disrupting the smuggling supply chains and identifying additional criminal activities within prisons, managed access and cell phone detection systems will better serve "law enforcement and corrections applications in Federal and State prison facilities" than wireless jammers. Before making any recommendations in this area, NTIA should fully investigate these superior alternative technologies.

---

18 *See* H.R. Conf. Rep. No. 111-336 (2009), Division B, Title 1, Page 619.

19 *Id.*

20 *See* Sanders & Johnk, *supra* note 5; Edward F. Drocella, Dept. of Commerce, NTIA, *Initial Assessment of the Potential Impact from a Jamming Transmitter on Selected In-Band and Out-of-Band Receivers*, NTIA Technical Memorandum 10-468 (May 2010).

IV. CONCLUSION

T-Mobile shares NTIA's concern about contraband cell phone use in prison facilities. The evidence suggests that smuggling of illicit cell phones into prisons has been on the rise and that these devices are used to facilitate illegal conduct. Wireless jammers are not an appropriate solution to this serious problem, however, because they would interfere with legitimate communications, including 9-1-1 calls and critical public safety communications, while also being ineffective at accomplishing the overall goal of preventing unauthorized wireless use. In terms of technological solutions, managed access and cell phone detection systems provide effective means of addressing the use of contraband mobile devices in prisons without the hazardous pitfalls associated with wireless jammers.

Respectfully submitted,

/S/ Kathleen O'Brien Ham

Kathleen O'Brien Ham
Eric Hagerson
T-Mobile USA, Inc.
401 9th Street
Suite 550
Washington, DC 20004

June 11, 2010