Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION
ADMINISTRATION
Washington, D.C.

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

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

Michael F. Altschul
Senior Vice President and General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Brian Josef
Director, Regulatory Affairs

CTIA-The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

Dated: June 11, 2010
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION AND SUMMARY</td>
<td>3</td>
</tr>
<tr>
<td>II. AS NOTED IN THE NOTICE OF INQUIRY, THE USE OF JAMMING TECHNOLOGY IS PROHIBITED FOR NON-FEDERAL ENTITIES</td>
<td>6</td>
</tr>
<tr>
<td>III. ALTERNATIVE TECHNOLOGIES SUCH AS MANAGED ACCESS AND CELL DETECTION SHOULD BE MORE ROBUSTLY INVESTIGATED</td>
<td>9</td>
</tr>
<tr>
<td>A. Managed Access Technology Allows for the Completion of Authorized Calls and the Collection of Information About Contraband Phones</td>
<td>10</td>
</tr>
<tr>
<td>B. Cell Detection Technology Enables Confiscation of Contraband Devices and Criminal Prosecution While Preventing Interference to Legitimate Use</td>
<td>13</td>
</tr>
<tr>
<td>C. The Alternative Technologies Proposed by the Industry and Corrections Departments Have Significant Advantages over Jamming</td>
<td>17</td>
</tr>
<tr>
<td>IV. CELL JAMMING, AS DEMONSTRATED BY NTIA TESTING, PRESENTS INTERFERENCE CONCERNS TO PUBLIC SAFETY AND COMMERCIAL NETWORKS</td>
<td>18</td>
</tr>
<tr>
<td>A. Effective Jamming in a Prison Necessitates “Overjamming” and Interference Outside the Prison</td>
<td>19</td>
</tr>
<tr>
<td>B. The Use of Jammers Will Harm Public Safety Operations</td>
<td>21</td>
</tr>
<tr>
<td>C. The Use of Jamming in Prisons Will Lead to an Increase in Unauthorized Jammer Use</td>
<td>23</td>
</tr>
<tr>
<td>D. There Is No Evidence That Jamming Technology Effectively Serves Its Intended Purpose</td>
<td>25</td>
</tr>
<tr>
<td>V. NTIA’S REVIEW MUST HOLISTICALLY ADDRESS THE FACT THAT WIRELESS USE IN PRISONS IS A CONTRABAND ISSUE AND CONSIDER ALL STEPS NECESSARY TO PREVENT THE SMUGGLING OF CELL PHONES INTO PRISONS</td>
<td>27</td>
</tr>
<tr>
<td>VI. CONCLUSION</td>
<td>31</td>
</tr>
</tbody>
</table>
Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C.

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

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

Between May 17 and May 20, 2010, there was a significant interference event in downtown Philadelphia that disrupted commercial wireless service and GPS signals and involved the joint efforts of the Coast Guard, the FCC, the NCS, and carriers. Due to inference from a jammer, GPS equipment failed to work and navigation aids (including those used by the Coast Guard and potentially the FAA) and timing synchronization based on GPS at wireless base stations were disrupted. Numerous CMRS base station sites completely lost the ability to make voice and data communications work, resulting in excessive blocked and dropped calls, and wireless providers and first responders relying upon GPS for 911 calls’ location information were adversely affected. This was due to a jammer.

On May 19, the FCC dispatched field agents to determine the source of the interference, while wireless carriers also worked to track down the source of the interference. After an investigation, the FCC agents identified the source of the interference: a single jamming device in a private apartment. Effects from this single jammer extended more than a mile from the apartment containing the device and disrupted signals throughout that area. The field agents shut the jammer down, but its
owner turned it back on the next morning before finally surrendering the equipment to the FCC later that day.

The incident in Philadelphia highlights an issue of critical importance to both the wireless industry and the Federal government: the use of wireless jammers and the devastating impact on commercial and Public Safety wireless services cannot and should not be tolerated. As American consumers and public safety officials increasingly rely on wireless communications, the ability of wireless networks to operate without harmful interference becomes even more vital. Wireless jammers represent a major threat to wireless networks and everyone else who relies on wireless communications.

For this reason, CTIA – The Wireless Association® (“CTIA”) respectfully submits these comments in response to the National Telecommunications and Information Administration (“NTIA”)’s Notice of Inquiry\(^1\) to stress the highly detrimental impact that one of the proposed technologies – jamming – has on commercial and Public Safety operations and to encourage the evaluation of alternative technologies, as well as a holistic approach to the contraband cell phone problem. CTIA strongly opposes the use of contraband cell phones in prisons and applauds NTIA’s commitment to preventing the use of contraband cell phones. Considering “the adverse effects” that jamming imposes on commercial wireless and Public Safety services in areas surrounding the prisons,\(^2\) CTIA believes that the focus should be on evaluating the multiple technologies that do not involve jamming and that will address the issue of contraband phones in prison.

---

\(^1\) \textit{Preventing Contraband Cell Phone Use in Prisons, Notice of Inquiry, 75 Fed. Reg. 26733 (May 12, 2010) (“NOI”).}

\(^2\) \textit{Id.} at 26734.
I. INTRODUCTION AND SUMMARY

The possession and use of contraband cell phones in correctional institutions is a mounting problem, and CTIA and its members strongly support resolution of this issue. However, CTIA stresses that this issue must be resolved in a manner that preserves the ability of law-abiding members of the public, as well as Public Safety personnel, to continue to reliably access wireless services.

Some parties have attempted to cast a single technology – wireless jamming – as the sole solution to controlling contraband phones in correctional institutions. But as H.L. Mencken famously noted, “[f]or every complex problem, there is a solution that is simple, neat, and wrong.” A clear record has emerged that jamming is not a panacea, but rather risks proving ineffective at stopping the use of contraband cell phones in prisons while posing a major threat to the proper functioning of commercial and Public Safety wireless services in and around prisons. For example, New Zealand recently invested more than $5 million to install jamming technology in the country’s 20 prisons, as well as $200,000 in annual support for the system.3 Even with the jammers in place, prisoners were able to place calls from within the prison over a new wireless network.4 Further, the smuggling of cell phones into prisons persisted after the jammers were installed.5

In addition to the Philadelphia jamming incident mentioned above, there have been countless other jamming incidents that have caused interference to Public Safety and commercial wireless networks as well as the GPS system. CTIA has attempted to


4 Id. (“The Dominion Post reported that a prisoner recently told the Parole Board that he used the 2degrees network to call his children.”).

5 Id.
categorize some of these incidents within these comments, but there can be no mistake –
widespread use of jamming technology by prisons will by its very nature lead to an ever
increasing number of these types of interference events.

CTIA believes that the current law recognizes the limitations and problems
presented by the use of jamming technology. As NTIA acknowledged in the Notice of
Inquiry, the use of jamming technology is currently prohibited for non-Federal entities. 6
While there is a limited exception to the Communications Act that permits Federal
entities to use jamming equipment, NTIA would be better served by focusing its efforts
on alternative, legal technologies that do not pose an interference risk to commercial
wireless and Public Safety networks, as Congress has directed.

In addition to referencing jamming, the Notice of Inquiry discusses two alternative
technologies: managed access and cell detection. CTIA urges NTIA to undertake a
robust investigation of these two alternative technologies, as they are (1) permitted under
existing laws, (2) effective in eliminating the use of contraband cell phones, and (3) do
not pose the same interference risk as jamming. In fact, cell detection and managed
access each have several advantages over jamming, and would better enable law
enforcement personnel to confiscate contraband handsets and/or investigate the criminal
activity that contraband cell phone use currently enables. Both of these technologies are
widely available today, and implementation of either would achieve NTIA’s policy
objectives and be consistent with the goals expressed by Congress to not interfere with
Public Safety and commercial wireless network operations.

6 Id.
CTIA supports managed access and cell detection over jamming because jamming presents grave interference concerns to Public Safety and commercial wireless networks. For a jamming device to effectively service an entire prison, prisons would be forced to operate jammers such that their impact is felt outside prison walls, causing interference to neighboring, legal wireless communications. The use of jammers also would have a severe detrimental impact on Public Safety and would block or degrade 911 calls from being completed, cause interference to dedicated Public Safety networks, inhibit the functioning of E-911 location accuracy, and prevent first responders from using wireless devices in emergency response within prisons. As Public Safety usage of commercial networks increases, and as Public Safety dedicated networks move closer to commercial networks in the spectrum bands, it is inconceivable that commercial use could be jammed without directly jamming public safety use. Further, enabling jamming in Federal prisons would cause the proliferation of illegal jammers into the stream of commerce for use elsewhere. The fact that jamming’s effectiveness is an unproven technology for combating the use of contraband phones further supports a finding that jamming should not be used in prisons.

Finally, while the Notice of Inquiry is primarily concerned with technical responses to the problem of contraband cell phone use in prisons, CTIA encourages NTIA to keep in mind the incentives that cause the smuggling of contraband phones to proliferate, and urges state and federal lawmakers to take steps that will impose harsher penalties for the possession, provision, or support of contraband handsets.
II. AS NOTED IN THE NOTICE OF INQUIRY, THE USE OF JAMMING TECHNOLOGY IS PROHIBITED FOR NON-FEDERAL ENTITIES

As NTIA correctly noted in the Notice of Inquiry, the operation of jamming devices by non-Federal entities is currently prohibited under the Communications Act of 1934, as amended (the “Act”). Specifically, Section 333 of the 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.” Consistent with this mandate, the Federal Communications Commission (“FCC” or “Commission”) has found that “[t]he intentional use of jammers is considered ‘malicious interference,’ which is strictly prohibited by the Communications Act of 1934, as amended, and by FCC Rules.” The Act, in Section 302, provides the Commission with the authority to enforce this mandate: Section 302(a) authorizes the Commission to adopt regulations to control the interference potential of radio frequency devices, while Section 302(b) prohibits the manufacture, import, and sale of equipment which does not comply with the Commission’s regulations promulgated under Section 302(a).

---

7 Id.
10 47 U.S.C. § 302a(a) (“The Commission may, consistent with the public interest, convenience, and necessity, make reasonable regulations (1) governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications . . .”).
11 47 U.S.C. § 302a(b) (“No person shall manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, which fail to comply with regulations promulgated pursuant to this section.”).
The Commission exercised its power under Section 302(a) of the Act to adopt Section 2.803, which prohibits the sale or use of equipment not certified by the FCC, as well as the sale or use of devices that cannot be certified by the Commission (i.e., devices that would violate the Communications Act or the Commission’s rules if operated).12 Relying in part on Section 2.803, the Commission has denied requests to conduct demonstrations of jamming equipment designed to block wireless telephone calls by prisoners, finding that “the proposed jamming . . . would be inconsistent with both the Communications Act and the Commission’s rules.”13

The FCC’s Enforcement Bureau also has affirmed the illegality of wireless jamming technology. In 2005, the Enforcement Bureau, relying on Sections 333 and 302 of the Act, stated that “the marketing, sale, or operation of [jamming equipment] is unlawful” and that “[a]nyone involved with such activities may be subject to forfeitures, fines, or even criminal prosecution.”14 Indeed, the Enforcement Bureau recently issued a Notice of Apparent Liability for Forfeiture to Phonejammer.com for marketing wireless device jammers in the United States, finding that “Phonejammer apparently willfully and

12 47 C.F.R. § 2.803. See also Letter from Kathryn Berthot, Enforcement Bureau, FCC to Shaker Hassan, Grand Trades Co., File No. EB-05-SE-059, Citation, DA 05-1622, at 4 (June 9, 2005) (citing 47 C.F.R. § 2.803(g) for the proposition that a “device such as a jammer which intentionally interferes with radio communications is not eligible for certification”).

13 Letter from James D. Schlichting, Acting Chief, Wireless Telecommunications Bureau, FCC to Devon Brown, Director, District of Columbia Department of Corrections, 24 FCC Rcd 2060 (Feb. 18, 2009). See also Letter from James D. Schlichting, Acting Chief, Wireless Telecommunications Bureau to Howard Melamed, CEO, CellAntenna Corporation, FCC WT Docket No. 09-30 (Mar. 17, 2009) (stating that “the proposed jamming at the Pine Prairie Correctional Center would be inconsistent with both the Communications Act and the Commission’s rules”).

14 Sale or Use of Transmitters Designed to prevent, Jam or Interfere with Cell Phone Communications is Prohibited in the United States, Public Notice, DA 05-1776 (June 27, 2005).
repeatedly violated Section 302(b) of the Act and Section 2.803 of the Rules by marketing two models of phone jammers in the United States.”

NTIA, therefore, has correctly acknowledged the illegality of operating jamming equipment, and it must not ignore this extensive history when evaluating technology solutions to prevent contraband cell phone use in prisons. While there is a limited exception to the legal prohibition on jamming that would enable NTIA to authorize jamming by federal users, NTIA should not exercise this authority to permit the use of jamming equipment in federal prisons.

Further, in late 2009 Congress acknowledged the detrimental effects caused by jamming technology when it instructed NTIA to conduct testing of technologies to prevent contraband cell phone use in prisons. Congress specifically instructed NTIA to evaluate “technologies that do not pose a risk of negatively affecting commercial wireless and public safety services in areas surrounding prisons.” This directive makes clear Congress’ intent that alternative technologies be demonstrated and that the preservation of service for commercial and Public Safety users could be jeopardized through the operation of jammers.

---


16 See 47 U.S.C. § 302(c) (“The provisions of this section shall not be applicable . . . to devices or home electronic equipment and systems for use by the Government of the United States or any agency thereof.”); 47 U.S.C. § 902(b)(2)(A) (granting NTIA the authority “to assign frequencies to radio stations or classes of radio stations belonging to and operated by the United States”); 47 C.F.R. § 2.807(d) (excluding from regulation under Section 2.803 [r]adiofrequency devices for use by the Government of the United States or any agency thereof” provided that this exception not be applicable to any device after it has been disposed of by such government or agency”).

CTIA applauds NTIA’s effort to eliminate contraband cell phone use in prisons. However, CTIA urges NTIA and the Commission to focus their attention on alternative, legal technologies that do not pose an interference risk to commercial wireless and Public Safety networks, rather than continue efforts on jamming technologies that would cause grave harm to commercial and Public Safety wireless users.

III. ALTERNATIVE TECHNOLOGIES SUCH AS MANAGED ACCESS AND CELL DETECTION SHOULD BE MORE ROBUSTLY INVESTIGATED

NTIA and the FCC should heed Congress’ stated preference for investigation of alternative technologies to combat contraband cell phone use in prisons, and CTIA welcomes the opportunity to comment on possible alternatives to the blunt instrument of wireless jamming. As the Department of Commerce has correctly observed, there “are other, possibly more effective, tools available to prison officials aside from those that jam all calls in a given radio channel.”

The Department of Commerce is correct. In fact, there exist alternative technologies that have a significant advantage over jamming, without the detrimental effects on legitimate, authorized communications.

CTIA and its member companies have been actively working with vendors of alternative technologies such as managed access and cell detection and submit that these alternative approaches are (1) permitted under existing laws, (2) effective in eliminating the use of contraband cell phones, and (3) capable of achieving Congress’ objectives without causing detrimental interference to Public Safety and wireless networks. Indeed, last year CTIA convened a day-long meeting involving North American vendors of cell

---

detection and managed access solutions, as well as engineers from several of CTIA’s member companies. CTIA also has engaged with the Maryland Department of Public Safety and Corrections to investigate and develop collaborative solutions. CTIA urges NTIA and the FCC to further investigate these technologies as an alternative to jamming.

A. Managed Access Technology Allows for the Completion of Authorized Calls and the Collection of Information About Contraband Phones.

As stated in the Notice of Inquiry, managed access technologies “intercept calls in order to allow corrections officials to prevent inmates from accessing carrier networks.” Specifically, a managed access solution would restrict communications on commercial wireless networks to only a subset of allowed users, with all other users in a designated area, such as a correctional facility, being redirected through the managed access system – and would block illicit calls from within the facility. Managed access solutions can use location determination-technologies to ensure that the controls apply only in the geographic area of the prison. And, “there is not even a claim that there is a material risk that the technology utilized could be easily, albeit unlawfully, transported for use in other locations, such as theaters, restaurants and hotels.”

19 Vendors in attendance included Airpatrol of Columbia, MD, BINJ Laboratories of Quincy, MA, Electronic Entities Group of Torrance, CA, ITT of Columbia, MD, Tecore Networks of Columbia, MD, CellAntenna of Coral Springs, FL, and Triple Dragon Communications of Vancouver, BC.

20 NOI at 26735.


22 Petition for Rulemaking of the Mississippi Department of Corrections, WT Docket No. 09-30, at 9 (“Aug. 21, 2009”) (“Mississippi Petition”).
Under managed access, when a call is made from a CMRS device located on prison grounds, the device recognizes the managed access system as the strongest signal, which enables the system to obtain information such as the device serial number, SIM card, or both.23 The managed access system would cross-reference this information against a database that indicates whether the device is unauthorized.24 If the system determines that the device is unauthorized, the managed access system does not permit the call to be completed and will either transmit a voice message to the caller, or direct the call to a designated official point of contact.25 Calls made from authorized devices will go through as intended.26 If a call is made to an unauthorized device in a correctional facility using a managed access system, the system will not allow the call to be completed. Rather, the caller may receive a recorded message. Regardless of whether a device is authorized or unauthorized, no 911 calls are blocked under a managed access framework.27

23 Id. at 6.

24 Id. (“[T]he Managed Access System cross-references that information against the Managed Access System’s database. This database, which is similar to a smaller version of the commercial carriers’ databases, is used to deny or allow services to process calls depending on whether the devices are authorized or unauthorized (which authorization determinations are made from information provided by prison officials.”).

25 Id. at 6-7

26 Tecore Networks, Intelligent Network Access: Precision Control of Communications in Secured Areas, at 3 (Nov. 2008) (“Tecore White Paper”), available at http://www.tecore.com/solutions/whitepaper.cfm#intelligent (“A ‘Known Good’ user is a subscriber that is configured in INAC as someone who is allowed cellular service and should be redirected to the commercial network. This redirection forces the handset to reattempt the location update that will occur on the commercial network. Once completed, this subscriber can use their device as normal for both inbound and outbound traffic. This results in a normal operation of commercial service for the subscriber while within the coverage area of INAC.”).

27 Mississippi Petition at 7.
For example, Tecore Networks’ Intelligent Network Access Controller (iNAC) “forms a radio frequency umbrella around a precisely defined target area and intercepts cellular devices within range,” enabling iNAC to terminate communication without requiring the retrieval of the contraband device.\footnote{Tecore Networks – iNAC Managed Access – Intelligent Network Access Controller, \textit{at} http://www.tecore.com/solutions/intellinac.cfm (last visited June 6, 2010).} Once a phone is taken outside the iNAC coverage area, the handset re-registers with its commercial network and is no longer under the managed access system’s control.\footnote{Tecore White Paper at 3.}

Thus, there are several advantages to deploying a managed access system to prevent contraband cell phone use in prisons: because managed access involves no transmission that jams a wireless signal, there is no interference to other users as a result of the managed access system’s operation; all 911 calls are permitted, wireless operations by facilities’ neighbors are not impacted, the managed access system does not drop roaming calls, Public Safety channels are not jammed, and authorized cell phone use within a correctional facility can continue as normal. Further, a managed access system can be set up such that inmates think their contraband phones are working normally, enabling law enforcement to collect the dialed number or even intercept the call. Indeed, as Tecore notes, a managed access system’s presence is not readily discernable to affected users:

While the subscriber handset is locked to the INAC, the display and appearance on the handset is the same as if they were on the commercial network. If the subscriber never uses their handset while in the INAC area, they may never realize the INAC exists. On the other hand, if a subscriber who is locked to the INAC, attempts to place a call or send a text message the attempt will fail as all attempts to use the INAC are denied. The user perception of the INAC takes advantage of some of the
typical frustrations any mobile phone user has experienced in normal operations. This further masks the purpose and operation of the equipment. Only after a repeated pattern of denial is established could the typical user discern the restricted access.\(^{30}\)

Managed access has received support and endorsement from the wireless industry and from corrections departments. The Wireless Communications Association, International noted that managed access or similar technical options “may provide an ideal solution: one that solves the contraband problem without causing harmful interference to legitimate wireless communications.”\(^{31}\) The Mississippi Department of Corrections has stated that “Managed Access Systems will provide an effective solution that can be quickly implemented to address the very serious, and sometimes deadly, problem of the illegal use of CMRS devices by inmates.”\(^{32}\)

### B. Cell Detection Technology Enables Confiscation of Contraband Devices and Criminal Prosecution While Preventing Interference to Legitimate Use.

Another alternative technology is cell detection, a monitoring and tracking approach that enables prison officials to identify individual wireless devices within the facility.\(^{33}\) Prison administrators and correctional officers can then locate and confiscate unauthorized wireless devices within the prison. By enabling confiscation of contraband devices, cell detection “can provide correctional authorities and law enforcement with call records, address information, and even photographs that can assist in disciplinary

\(^{30}\) Id.

\(^{31}\) 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).

\(^{32}\) Mississippi Petition at ii.

\(^{33}\) NOI at 26735.
actions and criminal prosecutions.\textsuperscript{34} Another option for prison officials is to leave the detected devices in place and monitor them in accordance with wiretap statutes.

Indeed, just over a year ago, monitoring of contraband prison cell phones in Baltimore led to the indictment on drug and weapons charges of 24 people – including four state prison officers – who “conduct[ed] cell phone conference calls to arrange business with inmates around the state.”\textsuperscript{35} By wiretapping known contraband cell phones, authorities were able to monitor criminal activity originating from within prison walls:

The court records read like a scene out of Goodfellas: From their prison cells and with the help of corrections staff, authorities say, members of a violent gang were feasting on salmon and shrimp, sipping Grey Goose vodka and puffing fine cigars - all while directing drug deals, extorting protection money from other inmates and arranging attacks on witnesses and rival gang members.\textsuperscript{36}

Cell detection technology is widely available today, with numerous companies offering solutions tailored toward curbing the use of contraband phones in prisons:

- AirPatrol Corporation’s Wireless Locator System monitors a specified area and “detects the location of Wi-Fi and cellular signals.”\textsuperscript{37} The Wireless Locator System contains a database that “logs start and stop times of calls, plus e-mails and other messages sent.”\textsuperscript{38}

\textsuperscript{34} Largent Senate Testimony at 3.


\textsuperscript{36} \textit{Id}.


\textsuperscript{38} \textit{Id}.
• BINJ Labs’ CellScan cell detection system “tracks each phone’s exact location, and if individuals move with their phones, CellScan indicates starting and ending positions.”
  
  CellScan was tested at the Washington, DC Department of Corrections, where CellScan “accurately detected 100 percent of the cell phones.”

• CellAntenna’s CJAM™ -- Cell Phone Detection and Control (CJAM-CPC) system “can detect the quantity of cell phones in a prison, identify their location, and determine which cellular provider the cell phone is connected to. A list of each cell phone’s serial number and which cellular provider they are connected to is created.” This system ensures “that only cell phones within a prison are targeted, and that communication in the surrounding community is not interfered in any way, including the ability to ignore public security cell phones within the prison.”

• Triple Dragon Communications’ DragonFire system locates illegal or unauthorized phones or track phones within a given restricted zone and disable targeted wireless devices, cutting off incoming or outgoing communications. DragonFire can also track the phone’s movement or the content of communications.

• The ORION NJE-4000 Non-Linear Junction Evaluator “detects semiconductor junctions . . . and provides a working solution to controlling contraband cellular phones in correctional facilities.” The NJE-4000 detects electronics in cell phones, even when the phone is turned off, and has been


40 Press Release, BINJ Labs, “CellScan testing a success in Washington, DC” (Aug. 3, 2006), available at http://binjlabs.com/news.html#press. CellScan’s system “uses complex arrays to detect cell phone signals (e.g. GSM, CDMA2000, TDMA, IS-95, etc.) as use occurs. The information is then clearly displayed on an electronic map of the facility to help practitioners locate the phones.”). Id.


42 Id.


44 Id.
used by the Tennessee Department of Corrections, the Georgia Department of Corrections, and the Estonian Department of Justice.

- The Cell Hound® from ITT “detects and locates all active cell phones located within or near a facility. The system utilizes an array of sensors that listen for cell phone activity. When a cellular call is detected, information about the call is transmitted via a standard Ethernet LAN to the central server. The data is processed in real-time by the software, which then displays the location of the cell phone onto a computer monitor.”

- Berkeley Varitronics Systems’ (“BVS”) Bloodhound Cell Detector was recently tested at a corrections facility in Maryland, where five contraband cell phones were confiscated. Of these phones, “two were on . . . active voice calls, one was being used for text messaging, and two were hidden on standby mode. One of the hidden phones was in a hollowed out brick covered by a capstone in a low wall that separates bunks areas in a dormitory. The second was inside an electrical box that had been covered with a solid utility plate that was held in place with security screws.” It took two hours for Maryland corrections officials to find these phones, and based on these results, the Maryland Division of Corrections plans “to place additional orders for the Bloodhound cell phone detector.” BVS also recently announced the release  

---


46 Press Release, Research Electronics International, “Georgia Department of Corrections Implements ORION NLJD to Locate Hidden Contraband Cellular Phones in Correctional Facilities” (Aug. 20, 2007) (“Feedback from the Georgia Department of Corrections has been very positive indicating that they have located multiple contraband cell phones as well as other electronic contraband using the ORION.”).


50 Id.
of a palm-sized cell detection device that vibrates when nearby cell phone
activity is detected.  

Not only have numerous companies developed effective, lawful cell detection
solutions, but the United States Department of Justice has acknowledged the need to
improve its ability “to detect, locate and defeat the use of unauthorized wireless
communications devices in all operating environments, including in, but not limited to,
correctional environments,” also adding that it requires “[i]mproved, unobtrusive means
to accurately detect a broad spectrum of contraband to preclude its introduction into
correctional . . . environments.”  

Cell detection technology helps meet these objectives while preserving authorized communications in and surrounding correctional facilities.

C. The Alternative Technologies Proposed by the Industry and
Corrections Departments Have Significant Advantages over
Jamming.

The above-cited examples of alternative technologies demonstrate that managed
access and cell detection contain functionalities that are not possible under a jamming
framework. Indeed, while jamming may thwart the use of contraband phones in some
cases, it will not prevent smuggling, identify the location of unauthorized devices, enable
the confiscation of contraband phones, or enable the management and possible
wiretapping of contraband phones for legitimate law enforcement purposes. Rather,
jamming is a blunt instrument that may not effectively jam all devices, and all signals all
of the time, and that precludes useful monitoring and contraband retrieval functions while

Releases Stealthy Cell Phone Detector” (June 2, 2010), available at

52 U.S. Department of Justice, National Institute of Justice, “High-Priority Criminal
causing harmful interference to legitimate wireless communications within prisons, as well as neighboring wireless users.

Alternative technologies also can change the incentives for contraband cell phones that currently exist: they reduce the value of contraband to those who provide it and reduce the value of cell phones to inmates. On the other hand, jamming may increase the scarcity of contraband cell phones, but will also increase the value of contraband and enable device smugglers to make an even heftier profit. This is because, as discussed below, jamming will not guarantee that contraband wireless devices will be rendered inoperable.

IV. THE NTIA TESTING OF JAMMING HIGHLIGHTS INTERFERENCE CONCERNS TO PUBLIC SAFETY AND COMMERCIAL NETWORKS

Not only are alternative technologies superior to jamming readily available, but jamming also is an unproven solution to the problem of contraband cell phones in prisons, and presents a grave interference threat to Public Safety and commercial wireless networks. Recent testing conducted by NTIA demonstrates these interference risks, while failing to prove the efficacy of jamming in curbing the use of contraband wireless devices. Further, permitting cell jamming in prisons will likely increase use of jammers by unauthorized persons as equipment intended for Federal users reaches the stream of commerce.

53 For example, the South Carolina Department of Public Safety has a mobile system with base stations on 857 and 858 MHz (interleaved with Specialized Mobile Radio frequencies).
A. Effective Jamming in a Prison Necessitates “Overjamming” and Interference Outside the Prison.

Jamming is an inexact methodology that does not distinguish between desirable and undesirable signals. As such, given the dynamic nature of wireless networks, it will be extraordinary difficult for jamming technology to be effective without causing significant harm. Wireless providers constantly strive to improve their network coverage and customers’ signal quality, which is impacted by changes in network load, cell tower locations, weather, and the time of year. Just as wireless providers constantly monitor and adjust their networks to best serve their customers, jamming providers must constantly monitor wireless signal strength and make corresponding changes to their technology to ensure that it remains effective – an unlikely outcome.

For jamming to be effective, correctional administrators will have to jam their entire facilities. Absent a commitment to jam the entire facility, inmates can easily learn where smuggled cell phones can be used outside the range of a jammer and may still be able to complete calls or send text messages. However, because wireless jamming signals cannot be confined to precise geographic boundaries, and because radio waves propagate in a non-linear way, jamming an entire facility will require “over-jamming” in which the harmful signal extends beyond the walls of the prison facility and into areas where legitimate users may experience harmful interference to their wireless communications. Recent testing conducted by NTIA confirms this fact:

The jammer emissions were transmitted entirely indoors. The targeted jamming zone was the interior of a two-floor reinforced cinderblock structure measuring 30 meters (m) long by 8 m wide. Jammer emissions were measured both indoors and outdoors, that is, both inside and outside the targeted jamming zone. . . . For the outdoor locations where jamming
was not intended, the results showed that jammer power was measurable at distances up to 127 m from the building.\textsuperscript{54}

It is clear, therefore, that “overjamming” is an inevitable outcome of the operation of jamming equipment in prisons.

Indeed, there have been numerous examples of harm to legitimate users caused by overjamming of prisons and other facilities, both in the U.S. and around the world. As CTIA has previously noted, a jamming device in a Brazilian prison knocked out wireless service to nearly 200,000 nearby residents.\textsuperscript{55} And in India, a jammer in a prison disrupted service to people living within a five-kilometer radius.\textsuperscript{56}

Similarly, the unauthorized use of cell phone jammers in non-prison facilities has caused interference to neighboring users in the United States and worldwide. At Mt. Spokane High School in Mead, Washington, school administrators installed an illegal jammer to prevent students from using cell phones during school hours, but this jammer also caused interference for the county sheriff’s cross-band repeater, a critical tool in enabling local Public Safety communications.\textsuperscript{57} In Auckland, New Zealand, a church


\textsuperscript{56} Madhuprasad N, Central prison forced to withdraw mobile jammers, Deacon Herald (May 13, 2006).

\textsuperscript{57} See Illegal Wireless Devices, Andrew Seybold Perspective (Mar. 10, 2009), available at http://andrewseybold.com/static/public/blog/blog244.html (“The idea was to prevent students from being able to use their cell phones during class for text or voice. However, when the jammer was turned on, it also jammed the radio that the Spokane County Sheriff had installed in the school that is used for both normal police activity and for swat teams that might be needed. The sheriff's quote went like this. ‘While I understand the problems / issues of teenagers and cell phones, interference to emergency communications is not acceptable. As I was not aware of this situation, I will be checking with the FCC enforcement bureau next week for any updates or information.’”).
was fined by the New Zealand Economic Development Ministry after it installed a jammer that “was interfering with cellular signals hundreds of feet from the church.”\textsuperscript{58} The Ministry observed that “the chances of emergency calls in the area failing thanks to the jammer were significant.”\textsuperscript{59}

The FCC’s recently-released National Broadband Plan has introduced another challenge to the efficacy of jammers. In recent years, several new spectrum bands such as AWS-1 and 700 MHz spectrum have been made available for commercial use.\textsuperscript{60} The National Broadband Plan has pledged to make an additional 500 MHz of spectrum available for commercial use.\textsuperscript{61} Whenever a new spectrum band is designated for terrestrial mobile services, prisons will need to update their jamming technology to ensure that all mobile devices’ signals are blocked, a highly expensive and likely infeasible undertaking.

\textbf{B. The Use of Jammers Will Harm Public Safety Operations.}

The use of jammers would have a particularly detrimental impact on Public Safety communications. Two leading Public Safety organizations, the Association for Public-Safety Communications Officers-International (“APCO”) and the National Emergency Number Association (“NENA”), have strenuously opposed the operation of


\textsuperscript{59} \textit{Id.}

\textsuperscript{60} Federal Communications Commission, Connecting America: The National Broadband Plan at 78 (2010).

\textsuperscript{61} \textit{Id.} at 84-89 (recommending that the Commission make 500 megahertz of spectrum available for mobile broadband over the next ten years, including 20 MHz of 2.3 GHz Wireless Communications Service spectrum, 10 MHz of Upper 700 MHz spectrum, up to 60 megahertz of Advanced Wireless Services spectrum, 90 megahertz of Mobile Satellite Spectrum, and 120 megahertz of broadcast television spectrum).
jammers. Because jammers block 911 calls, could cause interference to Public Safety networks, and inhibit first responders’ ability to communicate inside prisons, the use of jamming equipment poses a major Public Safety risk.

Unlike the alternative technologies discussed above, jammers block all calls – even calls to 911. APCO “is deeply concerned that the use of [jammers] will block 9-1-1 calls from wireless telephones.”62 Similarly NENA “is particularly concerned over the potential of wireless jamming technology for the blocking of 9-1-1 calls” and has stated its belief that there are other ways “to better balance the public interest in deterring criminal activity, on the one hand, and protecting lawful communications from interference on the other hand.”63 The recent incident in Philadelphia is a concrete example of the harm to Public Safety and commercial networks that jamming technology presents. Because wireless providers that rely upon GPS for location information for 911 calls were adversely affected, E-911 calls did not have as accurate location information to provide to Public Safety Answering Points.

APCO has also cited the risk that “creating a serious threat to the safety of life and property . . . [t]here is also a potential that these ‘cell phone jamming’ devices could also interfere with Public Safety radio communications in adjacent frequency bands.”64

Public safety networks are deployed in the 700 MHz and 800 MHz bands, which are adjacent to or near commercial wireless spectrum. There also are plans under


64 APCO Letter.
consideration where public safety officials would utilize commercial networks. Obviously to be effective, the jammers would have to jam these shared networks, causing harm to Public Safety communications. As such, technologies designed to jam commercial frequencies would likely cause out-of-band interference to dedicated Public Safety channels.

Finally, the presence of jamming equipment in prisons would greatly frustrate the efforts of Public Safety in the event of an emergency taking place inside prison walls. APCO has stressed that “[t]he potential of jamming outside of the environment of a prison . . . may also disrupt responders who may need to use these cellular data services in response to an issue within or around the prison campus.”65 There is always the possibility that first responders may have to enter a prison to fight a fire or deal with another emergency. These first responders would be unable to engage in critical communications if wireless devices inside the prison are jammed.

C. The Use of Jamming in Prisons Will Lead to an Increase in Unauthorized Jammer Use.

Another inevitable result of permitting the use of jammers in correctional facilities is the eventual presence of such equipment in the stream of commerce, where it could be used in an uncontrolled manner. If cell-jamming equipment is not destroyed once no longer in use, such devices could fall into the wrong hands.66 Indeed, this is


66 Id. at 6.
already occurring. For example, and as noted above, several schools have implemented jamming, even though schools are not authorized to use such equipment. In addition to the Washington case noted above, illegal jamming equipment was deployed by the Agate School District in Colorado that caused interference to a local carrier.\footnote{Largent Senate Testimony at 9.} Moreover, the recent Philadelphia jamming incident demonstrates the damage that a single jamming device can cause to both Public Safety and commercial wireless networks.

It is clear that jammers are entering the stream of commerce and are available to unauthorized users. The Commission recently issued a $25,000 fine against the manufacturer of a jammer installed in a Texas cosmetology school that caused interference to AT&T’s network.\footnote{Nate Anderson, \textit{Texas beauty school’s cell phone jammer leads to $25K fine}, Ars Technica, \textit{available at} http://arstechnica.com/tech-policy/news/2010/04/texas-beauty-schools-cell-phone-jammer-leads-to-25k-fine.ars (last visited June 6, 2010).} Similarly, Chinavasion Wholesale Electronics currently sells a cellular jammer hidden inside a painting that “effectively disables any cell phone” and “covertly and completely blocks mobile phone signals in an 80 meter radius.”\footnote{Chinavasion Wholesale Electronics, Painting Cell Phone Jammer, \textit{at} http://www.chinavasion.com/product_info.php/pName/painting-cell-phone-jammer/ (last visited June 6, 2010).} While Chinavasion warns potential buyers that “[t]his Product may not be permissible to import into certain countries,” it states that it will nonetheless “send you the product you order, however we will not accept any liability for customs issues arising from the ordering or usage of this device.”\footnote{\textit{Id.}} Cellular jammers will continue to proliferate and be used unlawfully if the technology experiences widespread adoption in corrections facilities.
D. There Is No Evidence That Jamming Technology Effectively Serves Its Intended Purpose.

The above-cited examples make clear the potentially devastating impact jamming has on authorized commercial and Public Safety wireless communications. Those reasons, coupled with Congress’s express preference for technologies that do not emit interference, make clear that jamming should not be considered as a solution to contraband cell phone use in prisons. Even recent NTIA testing did nothing to demonstrate that jamming is an effective solution. Indeed, there was no real measurement of the efficacy of jamming itself – while data was collected and recorded, the data itself was not conclusive.

Further, the testing conducted by NTIA was static – it did not replicate the dynamic, real-world effects and changes in wireless networks that constantly take place as a result of wireless providers’ monitoring and managing their networks. Changes in network topology, construction of new facilities, returning and rebanding, evolving usage patterns, new bands of spectrum coming on line, new devices, as well as simple things like changes in foliage over time would all impact the efficacy of jamming equipment. The results of NTIA’s testing were idiosyncratic to one facility and the jamming equipment used. Indeed, the testing report conceded that “[m]easurement of jammer emissions at other facilities would produce different results” and that “[v]ariations in

---

71 See supra note 17.

72 NTIA Report TR-10-466 at 22.
jammer characteristics, structural characteristics of buildings, and propagation factors will produce different results for different installations in different frequencies.  

NTIA’s testing also did not address the manpower required to monitor and oversee the impact of jamming on Federal, Public Safety, and commercial licensees. The widespread deployment of jamming technology will inevitably require significant monitoring and oversight to ensure that no harmful interference is caused to authorized wireless communications, but the test report does not explore this issue.

In fact, a recent trial of prison jamming in New Zealand casts further doubt on the efficacy of jamming as a solution to the use of contraband mobile phones in prisons. New Zealand invested more than $5 million to install jamming technology in the country’s 20 prisons, as well as $200,000 in annual support for the system. Even with the jammers in place, prisoners were able to place calls from within the prison over a new wireless network. Further, the smuggling of cell phones into prisons persisted after the jammers were installed.

In short, the positives of jamming are unproven, while the negatives are well documented and numerous. CTIA would additionally note that even though Federal authorities are permitted to deploy jammers, they have not. One can understand concerns

---


75 Id. ("The Dominion Post reported that a prisoner recently told the Parole Board that he used the 2degrees network to call his children.").

76 Id.
at the Federal level about the effectiveness of jamming technology and the corresponding issues surrounding this technology. Rather than continuing to explore use of this technology, CTIA instead encourages NTIA to look more carefully at legal technologies that show great promise in combating the issue of contraband cell phones within prison systems.

V. NTIA’S REVIEW MUST HOLISTICALLY ADDRESS THE FACT THAT WIRELESS USE IN PRISONS IS A CONTRABAND ISSUE AND CONSIDER ALL STEPS NECESSARY TO PREVENT THE SMUGGLING OF CELL PHONES INTO PRISONS.

Finally, while the Notice of Inquiry is primarily concerned with technical solutions to the problem of contraband cell phones in prisons, the fact remains that wireless use in prisons is fundamentally a contraband issue, and there are numerous other steps that can be taken to prevent this problem.

Congress, together with the states, needs to update and enforce their contraband statutes to impose tougher penalties for the possession, provision, or support of contraband wireless handsets. To properly address the contraband cell phone problem, Congress and the states must look to its source. It is widely acknowledged by prison officials that “the most common method used by the inmate population for obtaining cell phones is through the use of corrupted staff” at correctional institutions. Texas Inspector General John Moriarty acknowledged that “[t]here’s no question that corrupt officers are involved” in mobile phones moving into prisons and into the hands of

---

inmates.  Antonio Giola, who heads drug prosecutions at the Maryland State Attorney’s Office in Baltimore, affirmed this fact, stating that “[i]t’s not a big secret.  [Contraband Phones] are chiefly smuggled in by correctional officers.” Most recently, a former correctional officer was sentenced to two years in prison after pleading guilty to supplying drugs and a cell phone to an inmate at the Baltimore City Detention Center.

A successful approach to the phones-in-prisons problem, therefore, must examine the cause of behavior by prison officers. The motive for smuggling contraband cell phones into prisons is a financial one: over one year, one “correctional officer received approximately $150,000 for smuggling approximately 150 phones to inmates.” This correctional officer “was terminated, but there were no legal repercussions for his actions.” The California Office of Inspector General conceded that in general, “[e]mployees and contractors face minimal repercussions compared to the danger they create to other employees and inmates by supplying inmates with cell phones.”

It is clear, therefore, that states must significantly enhance the penalties associated with smuggling cell phones into prisons for this corruption to stop. These efforts must

---


79 Mike Hellgren, Calling the Shots: Cell Phones & Crime Behind Bars, available at http://wjz.com/local/cell.phone.contraband.2.999932.html


82 Id.

83 Id.
also extend to anyone who facilitates the use of contraband handsets by paying for associated wireless service. By extending liability to those who provide illicit wireless devices or enable their use by inmates, states will deter this behavior. Several states, including Arkansas, Florida, Indiana, Nevada, North Dakota, Texas, and West Virginia, have recently updated their contraband statutes to include specific penalties for the possession or provision of unauthorized handsets. Louisiana is currently considering a bill that would amend its definition of “contraband” to include component hardware of telecommunications equipment.\(^\text{84}\) CTIA encourages other states, as well as the Federal government, to enact legislation to make the possession, provision, or support of a contraband wireless device a felony.

CTIA also supports the Cell Phone Contraband Act of 2010, which was passed by the Senate and would prohibit the use or possession of cell phones and wireless devices in wireless prisons. Anyone who provides or attempts to provide an inmate with a cell phone could face imprisonment of up to one year.\(^\text{85}\) The bill also would require the Government Accountability Office to submit a report within 90 days of enactment on inmate phone use, including the rates they pay for landline service, the revenues of inmate phone systems, state and federal efforts to tackle the smuggling of mobile phones into prisons, and mobile phone use by inmates in prisons.\(^\text{86}\) The bill’s efforts to assess

---


the price of prison pay phones (which are under the control of corrections agencies) would be a major step toward reducing the value of cell phones to inmates, thus reducing incentives to smuggle the devices into prisons.
VI. CONCLUSION

CTIA believes that the illicit use of phones in prison must be stopped. But, for the reasons stated above, CTIA strenuously opposes the use of jamming equipment to combat contraband cell phone use in prisons. The potentially devastating impact of jamming on authorized commercial and Public Safety wireless communications makes it a highly inappropriate solution to the contraband phone problem, particularly when more effective, lawful alternative technologies already exist. CTIA urges NTIA to further explore the use of alternative technologies and holistically evaluate the contraband phone problem to determine how best to combat the smuggling of contraband phones into prisons.

Respectfully submitted,

By: Brian M. Josef

_______________________________
Brian M. Josef
Director, Regulatory Affairs

Michael F. Altschul
Senior Vice President and General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

CTIA-The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

June 11, 2010