BEFORE THE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
U.S. DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20005

In re	)	
	)	
Notice of Inquiry Regarding Preventing	)	Docket No. 100504212-0212-01
Contraband Cell Phone Use in Prisons	)	

COMMENTS OF AT&T Inc.

AT&T Inc., on behalf of itself and its affiliates ("AT&T"), hereby submits comments in response to the National Telecommunications and Information Administration's ("NTIA") Notice of Inquiry ("*NOI*") regarding possible solutions to prevent the use of contraband cell phones in prisons.[1] As NTIA documents, the illicit possession and use of wireless devices by inmates in correctional facilities is a genuine and important public safety issue.[2] Accordingly, AT&T strongly supports NTIA's efforts to prevent the use of contraband cell phones in prisons.[3] As detailed below, AT&T has concluded that managed network access solutions[4] show great

---

1 *Preventing Contraband Cell Phone Use in Prisons*, National Telecommunications and Information Administration, Notice of Inquiry, Docket No. 100504212-0212-01 (May 7, 2010) ("*NOI*").

2 *See id*. at 2 ("The use of contraband cell phones by inmates has risen as the U.S. prison population continues to expand.").

3 NTIA seeks comment on three broad categories of contraband cell phone intervention: managed network access, detection, and jamming. *See id*. at 3.

4 Managed access systems intercept calls in order to allow corrections officials to prevent inmates from accessing carrier networks. *See id*. at 5. The cell signal is not blocked by a jamming signal, but rather, is captured (or re-routed) and prevented from reaching the intended base station, thereby disallowing the completion of the call. *Id*. This technology permits calls by known users (*i.e.*, prison-authorized cell phone numbers) by handing them off to the network, and prevents others by denying access to the network. *Id*.

promise in preventing and controlling contraband cell phone use. In contrast, significant legal, technical, and policy concerns make jamming technologies unacceptable for use by prisons.

AT&T arrived at these conclusions after numerous interactions with prison officials, public safety officials, wireless providers, and equipment and systems manufacturers. AT&T is an active supporter of industry efforts to address contraband cell phones in prisons, including participating in a CTIA-sponsored test of technologies offering potential solutions to contraband cell phones in prison. In addition, AT&T continues to work closely with Tecore Networks ("Tecore"), a provider of managed network access solutions, to allow commercialization of managed access solutions in prisons. Tecore's managed network access solution shows great potential for addressing the problem of contraband cell phones without jeopardizing public safety and commercial communications.

In contrast, jamming technologies[5] raise significant legal and policy concerns that warrant serious and comprehensive consideration. As an initial matter, the use of jamming devices in state and local prisons violates the Communications Act, which prohibits the use of devices designed to interfere with or block wireless telephone calls.[6] Moreover, jamming is a blunt instrument that does not distinguish between desirable and undesirable signals,[7] and the effectiveness of jamming in controlling the use of contraband phones is an open issue. The disruptive impacts of jamming are not subject to precise geographic limitation and can extend

---

[5] Radio jamming is the deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of disrupting use of electronic devices, equipment, or systems—in this case, mobile devices such as cell phones. *See id*. at 4.

[6] *See* 47 U.S.C. §§ 301, 302(b), 333.

[7] *See* Declaration of Dr. Charles L. Jackson, Attachment B to CTIA's Petition for Reconsideration and Request for Referral to the Full Commission (Jan. 6, 2009).

outside prison grounds. Indeed, jamming may impact legitimate cell phone users adjacent to prison grounds, including public safety users and consumers.

AT&T cautions NTIA that none of the technological solutions proposed in the *NOI* offer a "silver bullet" that alone will eradicate contraband cell phones. Although new wireless technologies – such as the managed network access solution – show great potential to significantly reduce the problem, vigilant prevention and detection efforts by prison officials must remain the first line of defense.[8]

I. THE RISKS ASSOCIATED WITH A CELL JAMMING APPROACH TO CONTRABAND CELL PHONES IN PRISONS OUTWEIGH THE BENEFITS.

The legal and policy problems with jamming technology outweigh the benefits. As detailed below, the FCC has affirmed time and again that the Communications Act and the FCC's rules prohibit the jamming of cell phone signals. In addition to legal prohibitions, jamming technologies threaten legitimate public safety and commercial communications. NTIA and public safety agencies have expressed concern that consumers' signals may be jammed, rendering them incapable of making emergency calls. Jamming also may not be an effective way to preclude the use of contraband phones within every area of a large facility such as a prison. But nevertheless, jamming devices can block legitimate calls over large geographic areas, far beyond prison walls. Cell phone jamming is not an acceptable option in the fight against contraband cell phone use in prisons, particularly where other viable technological solutions exist.

---

[8] Although the *NOI* is limited to "RF-based, wireless technology solutions," NTIA recognizes that other contraband interdiction technologies may help to prevent the use of, or access to, contraband cell phones in prisons (such as x-rays, dogs, body scanning imagery, and other methods which detect contraband phones hidden on prison employees, visitors, and inmates). *NOI* at n. 12.

A. Jamming Cell Phone Signals is Prohibited Under the Communications Act and the FCC's Rules.

As a legal matter, jamming of cell phone signals is prohibited under the Communications Act and the FCC's rules. 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."[9] The jamming equipment discussed in the *NOI* falls within this general prohibition, for its sole purpose is to enable willful interference with licensed wireless transmissions. As the Commission has explained, "[t]he main purpose of . . . jammers is to block out or interfere with radio communications. Such use is clearly prohibited by section 333 of the Act."[10]

Jamming cell phone signals also violates Section 301, which 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."[11] For the reason set forth above, *i.e.* Section 333, wireless jamming equipment is not an "apparatus" susceptible of lawful operation "under and in accordance with this chapter."[12] Only AT&T and other wireless carriers hold "license[s] . . .

---

9 47 U.S.C. § 333.

10 *Monty Henry*, 23 FCC Rcd 8293, 8294 (May 27, 2008); *see also Victor McCormack*, 23 FCC Rcd 8264, 8265 (May 22, 2008); *Mr. Jean Pierre de Melo*, 22 FCC Rcd 20957, 20958 (Dec. 6, 2007); *Curtis King*, 22 FCC Rcd 19162, 19163 (Nov. 1, 2007); *Shaker Hassan*, 20 FCC Rcd 10605, 10606-7 (June 9, 2005).

11 47 U.S.C. § 301.

12 *Id*.

granted under the provisions of this chapter," and may therefore operate on their radiofrequencies.[13]

Section 302(b) also prohibits the use of cell phone jammers. Section 302(b) provides that "[n]o person shall . . . use devices . . . which fail to comply with regulations promulgated pursuant to this section."[14] The Commission has made clear that jamming equipment cannot be sold, marketed, or used consistent with Section 302(b) because the Section 333 prohibition on intentional interference renders such equipment ineligible for certification.[15] Furthermore, use of cell phone jammers directly violates the Commission's rules. Section 2.803(g) of the Commission's rules provides that "[s]uch devices shall not be operated, advertised, displayed, offered for sale or lease, sold or leased, or otherwise marketed absent a license."[16]

The FCC twice issued Public Notices re-affirming these authorities. In 1999, the Office of Engineering and Technology and the Compliance and Information Bureau issued a joint Public Notice stating:

> There are no provisions in the FCC's rules that permit the operation of any device intended to interfere with cellular communications. Further, Section 333 of the Communications Act, 47 U.S.C. 333, prohibits any person from willfully or maliciously interfering with the radio communications of any

---

13 *Id*.

14 47 U.S.C. § 302(b).

15 *See, e.g., Ms. Murina C. Bollaro*, 23 FCC Rcd 842, 843 (Jan. 28, 2008) ("Garden State has violated Section 302(b) of the Communications Act . . . by marketing in the United States radio frequency devices that are not eligible for certification."); *Monty Henry*, 23 FCC Rcd at 8294 ("[A] device such as a jammer which internationally interferes with radio communication is not eligible for certification.").

16 47 C.F.R. § 2.803(g).

> station licensed or authorized under the Communications Act or operated by the U.S. Government.[17]

The Public Notice further stated that "the operation of transmitters designed to jam cellular communications is a violation of 47 U.S.C. 301, 302(b), and 333,"[18] and concluded 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."[19] The FCC again addressed the issue in 2005, when "[i]n 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 "issu[ed] [a] Public Notice to make clear that the marketing, sale, or operation of this type of equipment is unlawful."[20]

These authorities have been affirmed yet again in recent FCC denials of requests to conduct jamming tests. The FCC's Wireless Telecommunications Bureau denied a request by the District of Columbia Department of Corrections to host a demonstration of wireless jamming technology, finding that the proposed jamming would violate Section 333 of the Communications Act and Section 2.803(a) of the Commission's rules.[21] The FCC also granted

---

17 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).

18 *Id*.

19 *Id*. at 6998.

20 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).

21 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) ("Schlichting Letter").

CTIA – the Wireless Association's Petition to Deny CellAntenna's request for special temporary authority to demonstrate its jammers at a correctional facility in Louisiana.[22] The FCC found that the demonstration would be inconsistent with both the Communications Act and the FCC's rules.[23]

A limited exception to Section 333's prohibition on jamming enables NTIA to authorize jamming by the federal users under its jurisdiction.[24] Despite this exception, NTIA should not exercise this authority to authorize the use of jamming equipment in federal prisons. As discussed below, jamming raises the substantial likelihood of interference to legitimate users, including public safety users and ordinary consumers, and more efficient mechanisms exist to curb the use of contraband cell phones in prisons.

B. Jammers Raise the Risk of Harmful Interference to Legitimate Users.

Jamming is a blunt instrument that does not distinguish between desirable and undesirable signals.[25] As a practical matter, this means that instead of discriminating between contraband and legitimate cell phones, jamming technologies disable both. NTIA recognizes

---

22 *See* Letter from Howard Melamed, CEO, CellAntenna Corp., to Marlene H. Dortch, Secretary, Federal Communications Commission (Mar. 3, 2009); Petition to Deny of CTIA – The Wireless Association (Mar. 13, 2009).

23 *See* Schlichting Letter *supra* note 21.

24 *See* 47 U.S.C. §§ 302(c), 902(b)(2)(A); 47 C.F.R. § 2.807(d); *NOI* at 26738. As the Commission has consistently acknowledged, neither this exception nor any similar exception extends to state entities. *E.g.*, *Monty Henry*, 23 FCC Rcd at 8295 (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"); *Ms. 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.") (footnotes omitted).

25 *See* Declaration of Dr. Charles L. Jackson, Attachment B to CTIA's Petition for Reconsideration and Request for Referral to the Full Commission (Jan. 6, 2009).

that jamming systems "produce unwanted signals outside of their intended operating bands and are not naturally confined to a prescribed area."[26] Further, NTIA explains that these "signals have the potential to produce interference to other radio services operating in numerous frequency bands (including Federal Government operations) and outside of the prison facility."[27]

Jamming of 911 calls and public safety communications is particularly troubling. The Association of Public-Safety Communications Officials-International, Inc. and the National Emergency Number Association have both expressed serious concern over the possibility of wireless jamming technology blocking 911 calls or interfering with public safety radio devices.[28] The *NOI* also recognizes that preventing jamming of 911 calls from cellular phones is of "paramount concern as more consumers rely on mobile devices."[29] As NTIA notes, "[j]amming radio signals in and around prisons cannot differentiate between normal cell phone traffic and 911 calls."[30]

The disruptive impacts of jamming are not subject to precise geographic limitations and could extend beyond the area of intended effect, impacting authorized users nearby. The potential for disruption can increase depending on the setting – for example, the potential for disruption may be much higher in a congested urban area. The use of such equipment in federal

---

26 *NOI* at 7.

27 *Id*.

28 Letter from Chris Fisher, President, Association of Public-Safety Communications Officials-International, Inc. to Acting Chairman Michael Copps, Federal Communications Commission (Mar. 13, 2009); Letter from Brian Fontes, CEO, National Emergency Number Association, to Acting Chairman Michael Copps, WT Docket No. 09-30 (Mar. 17, 2009).

29 *NOI* at 10.

30 *Id*.

and state prisons would increase the scale on which jamming occurs to an unacceptable level, increasing the likelihood that lawful signals would be blocked and degraded.

C. NTIA Testing and International Experiences Highlight the Dangers of Jammers.

The concerns discussed above are not hypothetical. For example, NTIA's own studies indicate that wireless users beyond the prison walls may be unintentionally and negatively impacted by interference caused by jamming technology. In one test, NTIA's Institute for Telecommunication Sciences ("ITS") laboratory performed emission spectrum measurements on a jammer operating temporarily at a minimum security prison operated by the Federal Bureau of Prisons. The study measured jamming power beyond the prison – where jamming was not intended – at distances up to 127 meters from the building.[31] And in another recent laboratory and field test, NTIA found that jammers – when operating at full power and jamming in the Cellular and PCS bands – could impact Federal land mobile radio receivers and Global Positioning System receivers in and around the prison facility.[32]

Furthermore, the harmful jamming witnessed in the NTIA studies likely understates the damage jammers would cause if deployed on a wider scale. While NTIA acknowledges that it conducted a static test, and the results are "idiosyncratic to the technical particulars of this jammer transmitter and the building in which its signal was radiated,"[33] none of the NTIA test results actually demonstrate the overall effectiveness of the jamming technology, especially if the requirement is to jam every square foot of the facility. As a result, the recent study results

---

[31] National Telecommunications Information Administration ("NTIA") Report TR-10-466, *Emission Measurements of a Cellular and PCS Jammer at a Prison Facility*, at xi (May 2010).

[32] NTIA Technical Memorandum 10-468, *Initial Assessment of the Potential Impact from a Jamming Transmitter on Selected In-Band and Out-of-Band Receivers* at 4-1 (May 2010).

[33] *Id*. at 4-2.

alone should not be relied upon as a justification for a new policy direction in favor of jamming.

Experience from abroad is also instructive on this point. Jamming equipment used in prisons in other countries is documented to have caused serious interference to commercial wireless subscribers.[34] As discussed below, other more efficient methods of addressing the problem of contraband cell phones in prison are available.

II. MANAGED NETWORK ACCESS SOLUTIONS CURRENTLY SHOW THE MOST PROMISE IN SOLVING THIS PROBLEM.

Managed 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. As mentioned above, AT&T is working with Tecore to deploy a managed network access solution to prevent the use of contraband cell phones in prisons. Tecore's solution – the "Intelligent Network Access Controller (iNAC)" – would serve as a unified gateway for all commercial cellular networks, and would receive all call attempts made in the strictly-defined target area of the prison.[35] This solution provides a system operator – in this case, the prison – with the capability to selectively permit or deny voice, text and data

---

[34] CTIA Petition to Deny at 7-8 (describing a situation in Brazil where jamming equipment blocked cell service to 200,000 people living nearby; a situation in India where use of jammers was terminated after the equipment jammed cell phone operations up to a radius of five kilometers; and a situation in Pakistan where jammers caused interference to users on GSM and other wireless phone systems) (internal cites omitted); *see also* "Bars of trouble: Cell phones in jail," Pittsburgh Post Gazette, Oct. 10, 2008, http://www.post-gazette.com/pg/08284/918854-85.stm (explaining that jamming at a Brazilian prison knocked out cell phone service for 200,000 nearby residents).

[35] "iNAC Managed Access," Tecore Networks, http://www.tecore.com/solutions/intellinac.cfm. Notably, this system has received industry support from "CTIA, the top four U.S. commercial mobile operators, and other carriers whose networks cover corrections facilities." *Id.*

communications from all devices that funnel into the iNAC.[36] The iNAC technology also captures information about the transmitting device (including location and serial number) and SIM card, as well as originating and terminating telephone numbers.[37]

Managed access technology offers a myriad of benefits.[38] *First*, unlike jammers, a managed access solution allows for normal operation of authorized phones on and nearby prison grounds – including cell phones used by prison officials.[39] This solution permits 911 calls from all devices, including unauthorized devices.[40]

Second, with a managed access solution, control of the licensed spectrum remains with the licensee as required by the Communications Act. Prior to operation of the iNAC, the

---

[36] AT&T anticipates that Tecore's technologies will continue to evolve to support new frequencies and technologies.

[37] The system has three modes of operation: (1) managed access, which allows authorized devices to complete calls on the commercial networks, holds communication from other devices, and maintains regulatory compliance with features such as 911; (2) cell detection, which allows all calls to be completed on the commercial networks while capturing SIM, device and call information; and (3) lockdown, in which no communications are allowed.

[38] *See NOI* §§ 1, 4. These benefits have manifested themselves in recent public tests. On September 3, 2009, the Maryland Department of Public Safety and Correctional Services hosted a cellular disruption demonstration at the decommissioned Maryland House of Correction in Jessup, Maryland. The demonstration tested various non-jamming technologies for their effectiveness within the correctional environment. Tecore successfully demonstrated that its system can control calls within a prison with no direct interference to AT&T's network. *See generally* "Office of Engineering and Technology Grants Experimental License for Demonstration of Cellphone Managed Access Technology at Maryland Correctional Facility," News Release (Sept. 1, 2009).

[39] A small possibility exists that the iNAC might block a legitimate call if it is located directly outside of the prison and is captured by the Tecore system. Nevertheless, this risk of blocking is significantly smaller than with a blunt jamming solution.

[40] As NTIA recognizes, recent testing of managed access systems shows that these types of non-jamming technology "could allow certain phones to operate and allow 911 calls to be processed." *NOI* at 5. Managed access systems can be selective and designed to ignore 911 calls (*i.e.*, letting them connect to the network), and detection systems typically use passive devices that do not affect transmission or reception. *Id*. at 10.

managed access provider must enter into a spectrum lease with the wireless licensee, in which the licensee can contractually retain the right to terminate the lease or take other action in the event of harmful interference outside the prison. Further, calls in progress on a wireless licensee's network that begin outside prison grounds will not inadvertently hand-off to the prison system's iNAC if the device passes prison grounds during the call.[41] This solution also requires that the system operator coordinate with wireless carriers to ensure that the iNAC system uses the least disruptive channels.

These attributes are important to NTIA. Indeed, the Administration has remarked that "[a]voiding interference to authorized cell phone reception … is a *critical element* in evaluating the various technologies" because "longstanding radio spectrum regulation principle, embodied in the Communications Act of 1934, is to preclude harmful interference and not to block access to or receipt of information transmitted wirelessly."[42] In contrast, jamming systems – "in addition to producing emissions in specific bands and within specific areas to deny service" – "also produce unwanted signals outside of their intended operating bands and are not naturally confined to a prescribed area."[43] And these "signals have the potential to produce interference to other radio services operating in numerous frequency bands (including Federal Government operations) and outside of the prison facility."[44] Indeed, jammers transmit across all frequencies to prevent cell phones from selecting a different control channel.

---

41 In contrast, jammers might drop lawful calls placed by individuals as they drive past prisons that use jamming equipment.

42 *NOI* at 7.

43 *Id*.

44 *Id*.

Third, the managed network access solution disrupts unauthorized communications before they occur. As noted above, the iNAC provides the system operator with the capability to selectively permit or deny communications from wireless devices before the communications reach the wireless licensee's network.

Fourth, the managed network access solution does not require prison personnel to retrieve devices to terminate communications. All calls funnel into the iNAC system, which is controlled by a system operator at the prison.

Fifth, the managed access solution helps facilitate detection of contraband devices. The iNAC solution provides prison officials with device and call information for forensic analysis, which can aid detection efforts.

Although the managed network access solution will prevent most communications from contraband cell phones,[45] vigilant prevention and detection efforts by prison officials must remain the first line of defense. Implementation of managed access systems supplemented with detection efforts would significantly advance efforts to prevent the use and possession of contraband cell phones in prisons.[46]

---

[45] The managed access solution is not foolproof. For example, inmates could transmit over Family Radio Service and General Mobile Radio Service frequencies, using analog, short range, line-of-sight devices. Although these communications would have limited utility to inmates, AT&T nevertheless acknowledges that a managed access system would not prevent such communications.

[46] Indeed, NTIA posits that "[i]n order to completely eradicate contraband cell phone use, the cell phone must be physically located and removed, which can be labor-intensive. Inmates may use them for a short period of time and turn them off and then move them, making the devices more difficult to locate." *NOI* at 11. Although managed network access solutions contain certain functionalities that aid detection efforts, "[j]amming cannot identify the specific location of a contraband cell phone." *Id*.

IV. CONCLUSION

For the foregoing reasons, managed network access solutions should form the foundation of NTIA's plans to prevent contraband cell phone use in prisons. Managed network access shows great promise in preventing contraband cell phone use without interfering with the rights of wireless licensees and their customers. In contrast, significant legal, technical, and policy concerns make jamming technologies unacceptable for use by prisons.

Respectfully submitted,

/s/

Bruce R. Byrd
AT&T Inc.
1133 21st Street, N.W.
Suite 900
Washington, D.C. 20036
Counsel for AT&T Inc.

June 11, 2010