

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

In the Matter of )  
 )  
Promoting Technological Solutions to Combat ) GN Docket No. 13-111  
Contraband Wireless Device Use in )  
Correctional Facilities )

**REPLY COMMENTS OF AT&T**

AT&T Inc. (AT&T), on behalf of its subsidiaries, respectfully submits these reply comments in the docket captioned above.<sup>1</sup>

All parties to this proceeding agree that the use of contraband wireless devices by inmates in correctional institutions is a threat to the safety of prison employees, other prisoners, and the general public. There is also broad agreement that prompt action is required to deal with this security threat. AT&T supports the use of either a managed access system or a detection system; both have proven useful without the harmful effects of jamming.<sup>2</sup> Indeed, AT&T and other wireless carriers have worked hard and contributed resources to make the deployment of managed access systems successful.<sup>3</sup>

---

<sup>1</sup> *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, *et al.*, Notice of Proposed Rulemaking, FCC 13-58 (2013) (“NPRM”).

<sup>2</sup> Some commenters continue to advocate for the use of illegal jammers in correctional facilities. *See e.g.*, Comments of Maryland Department of Public Safety and Corrections; Comments of American Correctional Association; Comments of Oklahoma Corrections Professionals. As explained in more detail below, such use would not only be unlawful but would endanger public safety and interfere with legitimate use of mobile wireless services.

<sup>3</sup> Suggestions that wireless providers have been uncooperative – or could be in the future – are unsupported by any evidence of such behavior. *See, e.g.* Comments of Marcus Spectrum Solutions, LLC at 14; Comments of Securus Technologies, Inc. at 4; 9.) These groundless accusations are an insufficient basis for the unnecessary regulations sought by some commenters in this proceeding. *See, e.g.* Marcus Spectrum Solutions, LLC at 30; NTCH, Inc. at 4 *et seq.*; Comments of Network Communications International Corp. at 2.

AT&T believes the issue of how to remove contraband devices from prisons, once they are identified, deserves further consideration. As AT&T explained in its comments, the FCC lacks the authority to invest prison officials with the power to order carriers to deactivate devices. Moreover, because detection systems are likely to identify not only contraband devices operated unlawfully within a correctional institution but also devices being operated lawfully within the institution or nearby that are not contraband devices, carriers who deactivate devices other than pursuant to a valid court order do so at considerable risk. Accordingly a rule purporting to allow prison officials to order carriers to shut off service to devices would not only be unlawful but contrary to the public interest.

### **Managed Access Systems**

Managed access systems are “are micro-cellular, private networks that analyze transmissions to and from wireless devices to determine whether the device is authorized or unauthorized for purposes of accessing public carrier networks.”<sup>4</sup> As such, they need to use a carrier’s licensed spectrum within the prison to attract the contraband device’s transmission to the managed access system. AT&T and other carriers have leased spectrum to managed access system operators for this purpose. Because ordinary spectrum leasing consumes time, the Commission proposed streamlining the leasing procedures for managed access systems.<sup>5</sup> AT&T and commenters interested in managed access supported these changes. AT&T also made two further suggestions.

First, because wireless providers have no ability to manage 911/E911 services when managed access systems are used within prisons, the Commission must make clear that wireless carriers are not liable in the event that a call to 911 is blocked, or E911 data is degraded, by a

---

<sup>4</sup> NPRM at ¶ 14.

<sup>5</sup> *Id.* at ¶ 24.

managed access system. Second, to streamline the leasing procedure further, the first lease entered into with a managed access carrier should become the “lead” application. Once approved, the carrier should need only amend the lease to add any new call signs, coordinates for the new license area and such other data the Commission may require.<sup>6</sup> This approach will save all parties — including the Commission — time, effort, and expense while still providing the information needed to track the leases.

The Boeing Company (“Boeing”), however, argued that spectrum leases are unnecessary for managed access systems and that the FCC has “ample authority to permit operation of managed access systems in prisons without a spectrum lease agreement.”<sup>7</sup> Boeing claims that the FCC “routinely authorizes operations in wireless carrier spectrum”<sup>8</sup> and cites a number of such instances that it claims supports its assertion. Whatever the merit of this argument— and AT&T does not regard it as meritorious, relevant or persuasive — it is simply the beard for Boeing’s real interest, which is unrelated to the matter at hand. That interest is Boeing’s desire to control, at some future point, mobile wireless spectrum within aircraft cabins.<sup>9</sup> Consequently, Boeing worries that “lease agreements to authorize managed access systems could create undesirable precedent”<sup>10</sup> as regards its plans for wireless devices on airplanes. In AT&T’s view, that worry is unfounded. More to the point, the proper place to raise this new proposal is in a proceeding in which the issue has been placed on public notice. Boeing’s proposal to allow the use of spectrum licensed to others without a license, lease or licensee consent is simply beyond the scope of

---

<sup>6</sup> The Commission should also waive its leasing rules to the extent necessary to allow licensees with site based authorizations, such as cellular, to enter into geographic area leases; i.e., leases covering license areas defined by lat/long descriptions, rather than site by site. This would allow a single exhibit describing the leased area to be used to cover all licenses to which the lease would apply for a given correctional institution.

<sup>7</sup> Comments of The Boeing Company at 5 (“Boeing Comments”).

<sup>8</sup> *Ibid.*

<sup>9</sup> *Id.* at 10.

<sup>10</sup> *Id.* at 9.

this one. The Commission should not divert time and attention away from the serious issue of prison security to deal with a matter of special pleading.

In any event, it is simply unthinkable that the Commission should permit the operation of another radio service within the exclusive licensed spectrum of a mobile wireless services provider without consulting that provider. Hundreds of millions of Americans rely on mobile wireless services to conduct business, stay in touch with family and friends, and to report emergencies. Any proposal to share this spectrum threatens the potential disruption of this vital radio-based communication service. The Commission's proposal here to refine spectrum leasing procedures strikes the right balance between protecting wireless networks and facilitating cooperation between mobile licensees and corrections officials in addressing the problems of the unlawful use of mobile devices smuggled into prison facilities.

### **Detection Systems**

Detection systems use passive, receive only technology to locate contraband devices within a prison. While prison officials could confiscate the device once located, they prefer, for several reasons, to have the carrier terminate service to the device. As CTIA noted in its comments, a requirement that wireless providers terminate service to the device at the request of prison officials raises "complex issues" for wireless carriers.<sup>11</sup> The Commission lacks authority to invest prison officials — or any other third person, not affiliated with the FCC<sup>12</sup> — with the power to order a carrier to terminate service to a device. Without a lawful termination order, carriers who mistakenly deactivate a legitimate account must bear the consequences of the termina-

---

<sup>11</sup> Comments of CTIA at 6.

<sup>12</sup> Comments of AT&T at 7. Even if the FCC possessed the authority to "deputize" state officials, CTIA notes that the term "qualifying authority," which is used in the FCC's proposed rule § 20.21, is vague and would create uncertainty for carriers as to the proper state official empowered to issue a termination order. CTIA Comments at 12.

tion, which may endanger the safety of a law-abiding user, engender disputes, and create potential liability and reputational harm.

This leads to a second point; namely, there needs to be a validation process that assures the cell detection system is working properly and affords the carrier the opportunity to confirm the accuracy of the termination information. Carriers should confirm this information because they are ultimately responsible for the termination, and they are well placed to determine whether a device identified as “contraband” has been mistakenly caught or misidentified by a detection system.

### **The Use of Jammers Would be Unlawful and Contrary to the Public Interest**

Many law enforcement commenters favor jamming as a means to repress the use of contraband wireless devices in prisons. However, the willful interference to radio communications of any U.S.-licensed radio station is, with few exceptions, forbidden by the Communications Act of 1934.<sup>13</sup> Jammers, by their very nature, cannot distinguish between contraband devices and legitimate devices, including devices used for alarm signaling/monitoring and those used for 9-1-1 calls.<sup>14</sup> As the FCC has noted

Use of jamming devices can place you or other people in danger. For instance, jammers can prevent 9-1-1 and other emergency phone calls from getting through or interfere with law enforcement communications (ambulance, fire, police, etc). In order to protect the public and ensure access to emergency and other communications services, without interference, the FCC strictly prohibits the use, marketing, manufacture, and sale of jammers.<sup>15</sup>

Moreover, given that radio propagation is an inexact science, there can be no assurance that a jamming system will block all illicit transmissions and not interfere with lawful radio communications. The routine use of jamming at correctional sites creates a genuine risk that important,

---

<sup>13</sup> 47 U.S.C. § 333.

<sup>14</sup> Comments of Alarm Industry Communications Committee at 2.

<sup>15</sup> *CONSUMERS BEWARE: It is Unlawful to Use “Cell Jammers” and Other Equipment that Blocks, Jams, or Interferes with Authorized Radio Communications in the U.S.* DA 11-250.

emergency calls will not be completed. It may also induce a false sense of security. A government report gives credence to these objections to the use of jammers in prisons.

In 2009, Congress directed the National Telecommunications and Information Administration (“NTIA”) and others to investigate and evaluate wireless jamming, detection, and other technologies that might be used to prevent contraband cell phone use by prison inmates. In 2010, NTIA published the report,<sup>16</sup> which, among other things, found several problems with jamming as a technology to prevent use of contraband wireless devices in prisons. The report noted that

- To prevent over-jamming, RF site engineering and extensive testing are required. This will increase the expense of a jamming solution
- Jamming signals are indiscriminate and will block legitimate emergency calls contrary to FCC rules.
- The use of jammers is illegal, even by prison officials.
- There is no Interference Protection Criteria (IPC) value for mobile phones and the industry would have to come to agreement on one if the law banning jamming were changed
- Incomplete areas of coverage in which prisoners have access to cell phones could lead to the prisoners identifying and exploiting dead-zones.
- Jamming that is limited to specific bands and technologies could lead to inmates selecting certain technologies and service providers as the technology-of-choice.<sup>17</sup>

Taken together, these financial, technical, legal and operational problems mean that the use of jammers in prisons will not occur for years, if ever.

For all these reasons, and the lack of certainty that a jamming system will actually achieve its goals, AT&T firmly opposes the use of jammers as both unlawful and contrary to the

---

<sup>16</sup> *Contraband Cell Phones in Prisons, Possible Wireless Technology Solutions*, U.S. Department of Commerce (December 2010) available at

[http://www.ntia.doc.gov/files/ntia/publications/contrabandcellphonereport\\_december2010.pdf](http://www.ntia.doc.gov/files/ntia/publications/contrabandcellphonereport_december2010.pdf)

<sup>17</sup> *Id.* at 18.

public interest. AT&T, therefore, urges the Commission, at the end of this proceeding, to dismiss those petitions seeking authority to operate jammers in the wireless communication bands.<sup>18</sup>

### **Conclusion**

For the foregoing reasons, AT&T respectfully urges the Commission to adopt the streamlined licensing procedures it has proposed in this NPRM as well as AT&T's additional suggestions. In addition, the interference protections proposed by AT&T should also be adopted. AT&T also urges the Commission not to require carriers to act on the termination orders issued by prison officials. The Commission cannot delegate this authority and carriers need to verify, to the extent possible, the accuracy of such a request. Finally, the ban on the use of jammers should continue in light of the serious threat of harm that their use presents to the legitimate use of mobile wireless services.

Respectfully submitted,



William L. Roughton, Jr.  
Michael P. Goggin  
Gary L. Phillips  
Margaret E. Garber  
AT&T SERVICES, INC.  
1120 20th Street, NW  
Washington, DC 20036  
(202) 457-2040 (phone)  
Counsel for AT&T Inc.

August 23, 2013

---

<sup>18</sup> Network Communications International Corp. ("NCIC") proposes the creation of "Quiet Zones" around prison facilities. Comments of NCIC at 2. This proposal deserves no serious consideration. As NCIC admits, declaring prisons to be "quiet zones" simply shifts the problem from prisons to wireless providers. *Id.* While the proposal would allow for scapegoating, there is no guarantee that this approach would constructively address the illegal possession and use of contraband devices in prisons. Indeed, it may be more likely to simply spark a new and brisk business in signal boosters or other technologies to evade the "quiet zone." In addition, like a jammer, a quiet zone would prevent the completion of legitimate wireless emergency calls from the prison and the vicinity. In short, this "solution" is just as unworkable as the use of jammers. The FCC should reject it for these reasons.