

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

In the Matter of

Promoting Technological Solutions to Combat  
Contraband Wireless Device Use in Correctional  
Facilities

)  
)  
)  
)  
)  
)

GN Docket No. 13-111

**REPLY COMMENTS OF AT&T SERVICES, INC.**

Jessica B. Lyons  
Michael P. Goggin  
Gary L. Phillips  
David L. Lawson  
AT&T SERVICES, INC.  
1120 20<sup>th</sup> Street, NW  
Washington, DC 20036  
(202) 457-2100

July 17, 2017

*Its Attorneys*

## TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY .....	1
II.	THE RECORD SUPPORTS A QUALIFYING REQUEST MECHANISM THAT PROVIDES CERTAINTY TO STAKEHOLDERS AND PROTECTS LAWFUL USE..	3
A.	Parties Support the Use of Judicial Processes.....	3
B.	A Qualifying Request Must be Well-Vetted and Accurate .....	6
C.	AT&T Supports a Certification Requirement for Contraband Interdiction Systems .....	7
D.	The Source of a Qualifying Request Should be Carefully Defined.....	9
III.	THE COMMISSION SHOULD NOT ADOPT A DEVICE DISABLING REQUIREMENT .....	10
IV.	ANY TECHNICAL SOLUTION MUST BE TECHNOLOGY NEUTRAL AND NOT HARM WIRELESS NETWORKS OR USERS .....	15
A.	Proposals to Require Beaconing Technology Violate Principles of Technological Neutrality .....	15
B.	Mandated Quiet Zones Would Frustrate Network Design and Degrade Service Quality Near Correctional Facilities .....	18
C.	Jamming Technology is Prohibited by the Communications Act, Harmful to Lawful Wireless Users, and Counterproductive .....	21
V.	CONCLUSION.....	25

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

In the Matter of

Promoting Technological Solutions to Combat  
Contraband Wireless Device Use in Correctional  
Facilities

)  
)  
)  
)  
)  
)

GN Docket No. 13-111

**REPLY COMMENTS OF AT&T SERVICES, INC.**

**I. INTRODUCTION AND SUMMARY**

AT&T Services, Inc., on behalf of its affiliates, (“AT&T”) hereby submits these reply comments in response to the *Further Notice of Proposed Rulemaking* (“*Further Notice*”) in the above-captioned proceeding.<sup>1</sup> The record developed in opening comments makes clear not only that the wireless industry is committed to combatting the use of contraband wireless devices by inmates in correctional facilities, but also that this effort is incredibly complex. AT&T has devoted considerable time and resources to supporting the deployment of contraband interdiction systems (“CIS”) such as managed access systems, as well as working with the Commission to develop a solution to the contraband phones problem. In adopting rules aimed at increasing the efficacy of CIS, the Commission must strike a careful balance: the rules must be reflective of technical realities, be consistent with the Communications Act and other laws, target unlawful uses with specificity, and – critically – protect lawful users of wireless services.

---

<sup>1</sup> *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Report and Order and Further Notice of Proposed Rulemaking, FCC 17-25 (2017) (“*Further Notice*”).

The *Further Notice* centered on a proposed process under which wireless providers would be required to terminate service to or disable contraband wireless devices once they have been identified.<sup>2</sup> For such a process to be successful, it will need to provide certainty to all affected parties and protect lawful uses. Commenters agree with AT&T that the best means of ensuring that a “qualifying request” accurately identifies contraband devices (and does not inadvertently affect lawful users) is to require a court order, in accordance with customary law enforcement processes. As a more general matter, AT&T agrees with other stakeholders that the Commission should certify any CIS used to generate qualifying requests, and that the source of a qualifying request should be carefully chosen. By taking these steps, the Commission will help ensure that qualifying requests are accurate and effectively executed.

AT&T also echoes those commenters who oppose a requirement that devices be completely disabled by a wireless carrier. Instead, at most the Commission should require that service be terminated to an identified device. As commenters observe, a device disabling requirement is technically infeasible in the near term, and would take years to implement. Even then, inmates would be able to circumvent the Commission’s rules by using outdated technologies.

Finally, any solution must be technology neutral and not harm wireless networks or lawful users. To mandate beaconing technology, as some suggest, would violate the Commission’s long-standing policy of technological neutrality and would likely have numerous negative consequences. Similarly, the Commission should not require after-the-fact “quiet zones” around correctional facilities, as such quiet zones would inhibit network design and

---

<sup>2</sup> *Id.* at ¶ 83.

degrade wireless service for lawful users near correctional facilities. To allow the use of jamming devices, as some suggest, would be not only unlawful, but also would harm lawful wireless users while not solving the problem of contraband phones in prisons. The Commission has consistently protected the public from the use of jammers in the United States, and should continue to do so.

## **II. THE RECORD SUPPORTS A QUALIFYING REQUEST MECHANISM THAT PROVIDES CERTAINTY TO STAKEHOLDERS AND PROTECTS LAWFUL USE**

The primary focus of the *Further Notice* is a process under which wireless carriers would be required to terminate service to or disable a device upon receipt of a qualifying request from an authorized party.<sup>3</sup> These qualifying requests would be based on the information gathered by CISs.<sup>4</sup> The most effective way to implement this system is to use judicial processes. The record contains ample support for a requirement that a court order be a condition precedent to any obligation by a wireless carrier to terminate service to and/or deactivate a device. As a more general matter, parties agree that there must be requirements in place to ensure the accuracy of qualifying requests and to protect lawful users of wireless services.

### **A. Parties Support the Use of Judicial Processes**

The most effective way to cut off the use of contraband phones while protecting lawful users is to require law enforcement to get a court order requiring a carrier to discontinue service to the devices identified. This process can be expected to ensure a high degree of accuracy in the list of contraband devices identified, is familiar to law enforcement and wireless carriers, will

---

<sup>3</sup> *Further Notice* at ¶ 87.

<sup>4</sup> *Id.*

help enforce criminal laws relating to contraband phone use, and will protect lawful users of wireless service.<sup>5</sup> Other commenters agree, and explain further the key role judicial processes can play in combating contraband phone use.<sup>6</sup>

Commenters agree that a court order requirement will ensure that a list of identified contraband devices meets an appropriate evidentiary threshold, protecting lawful wireless users and identifying with specificity devices that truly are contraband. As T-Mobile observes, “[w]ithout the check of judicial review, mistakes are more likely.”<sup>7</sup> Conversely, “a court’s evidentiary standards compel the party seeking injunctive action to have a valid factual basis for the request.”<sup>8</sup> The evidentiary finding supporting a court order – as well as the judicial processes required to obtain one – will provide assurances to all parties that only prohibited uses have been targeted.<sup>9</sup> As AT&T explained in its opening comments, it is essential that any qualifying

---

<sup>5</sup> Comments of AT&T Services, Inc., GN Docket No. 13-111, at 9 (June 19, 2017) (“AT&T Comments”).

<sup>6</sup> Comments of CTIA, GN Docket No. 13-111, at 5-6 (“CTIA Comments”) (“As CTIA has noted before, a court order directing wireless providers to prevent use of a wireless device is the soundest means of addressing the contraband device issue. This approach would ensure a high standard for such requests, provide for due process, and implement an effective enforcement mechanism in those states that prohibit use of contraband devices in correctional facilities.”) (footnotes omitted); Comments of Verizon, GN Docket No. 13-111, at 4 (June 19, 2017) (“Verizon Comments”) (“Court orders work because: a court’s evidentiary standards compel the party seeking injunctive active to have a valid factual basis for the request; service providers already have procedures in place that can be adapted to handle requests such as these; and the service provider does not face criminal or civil liability for implementing the request.”).

<sup>7</sup> Comments of T-Mobile USA, Inc., GN Docket No. 13-111, at 6 (June 19, 2017) (“T-Mobile Comments”).

<sup>8</sup> Verizon Comments at 4. *See also* Comments of CTIA, GN Docket No. 13-111, at 5-6 (“CTIA Comments”) (“This approach would ensure a high standard for such requests...”).

<sup>9</sup> T-Mobile Comments at 5-6 (“In these instances, a court of competent jurisdiction reviews evidence offered by an agency and determines whether the weight of evidence of illegal activity outweighs the customer’s right to privacy and non-interference by the government. The judges

request process have a high standard for accuracy and not wrongfully implicate law-abiding users.

By adopting a court order process, the Commission will also permit wireless carriers and law enforcement to leverage existing resources and expertise, and to facilitate enforcement of existing state laws. The problem of contraband cell phones in prisons is not a new or unique problem for law enforcement, and there is a long history of law enforcement using a court order process to gain access to records or otherwise prevent the use of communications devices. To date, however, the law enforcement community connected to the prison system has not taken advantage of these processes with respect to contraband phones. That should change. The majority of states have adopted criminal laws prohibiting the possession and/or use of wireless devices by inmates in correctional facilities, it is logical that law enforcement and judicial procedures be used in combating the presence of contraband phones.<sup>10</sup> This will also serve to

---

and prosecutors who participate in this process are officers of the court who have a legal responsibility to carry out their duties in accordance with the governing statutes. The statutory formalities and the judicial process in which they operate provide necessary assurances to the carriers that the requested actions are authorized by law.”).

<sup>10</sup> See, e.g., Letter from Daniel R. Hackett, ShawnTech Communications, Inc., to Marlene H. Dortch, Federal Communications Commission, GN Docket No. 13-111, at 3 (June 19, 2017) (“ShawnTech Comments”) (“[ShawnTech] is not opposed to DFCO participation per se, but depending on the type and location of the facility, such participation might invoke state laws as well as other federal laws for compliance purposes. By way of example and not limitation, termination might be inappropriate and possibly illegal within a CF if a state law crime has not been committed. This will obviously vary by state.”); T-Mobile Comments at 5 (“Requiring a court order would be consistent with the checks and balances traditionally imposed by the government when alleged illegal activity is suspected. For example, Federal statutes specify how and when a carrier can access a customer account on behalf of a government entity. In every instance, a legal demand is required. For the highest level of access, Federal statutes require the government to obtain a search warrant or court order.”).

protect all parties from liability in the event the qualifying request results in a lawful user's service being terminated in error.<sup>11</sup>

## **B. A Qualifying Request Must be Well-Vetted and Accurate**

Commenters agree that with or without a court order, any qualifying request must be well-vetted and accurate to ensure that lawful wireless users are not erroneously captured and their service disrupted. Not only would it be inequitable to terminate authorized communications, but doing so also poses a grave public safety risk.<sup>12</sup> Indeed, as the Internet of Things continues to proliferate, the public safety risks associated with inaccurate qualifying requests will increase.<sup>13</sup> For this reason, the party issuing a qualifying request should provide

---

<sup>11</sup> See, e.g., Comments of Prelude Communications, GN Docket No. 13-111, at 2 (April 28, 2017) ("Prelude Comments") ("We as a technology provider of CIS and Provider of Service to correctional agencies support the CMRS concerns about liability and privacy related concerns. The FCC should adopt rules ensuring CMRS, CIS and Provider of Service are protected from liability and legal issues related to the identification, capture and denial of service of wireless communication devices captured in the course of normal operations at a correctional/law enforcement facility.").

<sup>12</sup> Cell Command Inc.'s Comments in Response to the Commission's Further Notice or Proposed Rulemaking, GN Docket No. 13-111, at 5-6 (July 19, 2017) ("Cell Command Comments") ("For both legal and practical reasons, the adopted solution cannot interfere with devices external to the correctional facilities. Such interference would be illegal and, moreover, would potentially create a separate public safety concern by disabling or hampering the wireless devices of citizens residing in proximity to the correctional facility."); T-Mobile Comments at 2 ("As the Commission now considers additional rule changes, however, it must preserve the ability of the public to make and receive legitimate calls, especially those to emergency personnel. This includes legitimate calls placed in the vicinity of a correctional facility, as well as emergency calls from within a correctional facility."); Verizon Comments at 5 ("If the Commission decides that service termination is an appropriate way to address contraband devices, it should supplement the appropriate quality control safeguards proposed in the *Further Notice* to minimize the risk of an erroneous request terminating service to a legitimate user.").

<sup>13</sup> See T-Mobile Comments at n. 13 ("The Commission should also consider how, absent judicial review, termination of service requests would heighten the risk of accidental negative impacts on wirelessly connected devices other than phones, such as tablets or Internet of Things-



detailed information regarding the devices identified, the evidentiary basis for identifying the device as contraband, and the steps taken to ensure that lawful uses were excluded.<sup>14</sup> As explained further below, the party issuing the qualifying request should be required to make various certifications that will help ensure the underlying accuracy of the request. In the absence of a court's finding of sufficient evidence, these safeguards will help promote accuracy in the qualifying request process, to the benefit of all stakeholders.

### **C. AT&T Supports a Certification Requirement for Contraband Interdiction Systems**

AT&T supports proposals that require Commission certification of CISs as a condition precedent to any requirement by wireless providers to terminate service.<sup>15</sup> As AT&T made clear in its initial comments, the accuracy of a qualifying request is a paramount concern, and a certification requirement will help ensure that a CIS uses sound technology and only captures truly unauthorized uses. Specifically, before a CIS' findings may be used as the basis for a qualifying request, the CIS should receive certification under Part 2 of the Commission's rules and meet certain performance standards to be defined by the Commission. In addition, the Commission should publish and maintain a list of CISs that have met these certification requirements.

By requiring that CISs be certified under Part 2, the Commission will help ensure that CISs will not interfere with lawful uses. In the *Further Notice*, the Commission adopted a broad

---

based medical devices. The possibility of erroneously shutting off a connected medical device further underscores the need for judicial scrutiny of any termination of service order.”).

<sup>14</sup> See, e.g., T-Mobile Comments at 9.

<sup>15</sup> See, e.g., CTIA Comments at 5-6; ShawnTech Comments at 2; T-Mobile Comments at 8-9; Verizon Comments at 6.

definition of “contraband interdiction system” to be inclusive of a variety of technologies.<sup>16</sup>

Obviously, any frequency-emitting device must be certified under Part 2 to ensure that it does not cause interference. However, AT&T also agrees with CTIA that because even passive cell detection systems have the potential to produce emissions, all cell detection equipment should be certified under Part 2.<sup>17</sup>

In addition, the Commission should adopt certification criteria specific to a CIS, with the aim of ensuring that contraband interdiction systems produce accurate results. As AT&T and others emphasize in their opening comments, there are myriad harms associated with over-inclusiveness or inaccuracy on the part of a CIS. Thus, it is essential that quality controls be in place to prevent a CIS from blocking legitimate calls. AT&T agrees with T-Mobile that “[t]he certification process should be based on precise technical and performance standards designed to ensure the accuracy of the CIS and to prevent interference to service and devices beyond the confines of a correctional facility.”<sup>18</sup> This position has substantial record support.<sup>19</sup> AT&T also agrees that the Commission should maintain a list of certified CISs so that wireless carriers can

---

<sup>16</sup> *Further Notice* at ¶ 19.

<sup>17</sup> CTIA Comments at 5.

<sup>18</sup> T-Mobile Comments at 8.

<sup>19</sup> CTIA Comments at 5 (“The Further Notice properly recognizes that the systems used to detect contraband wireless devices and trigger a demand to restrict use of those devices must meet certain performance standards, and be deemed eligible by the Commission, in order to minimize the risk of preventing use of an authorized wireless device.”); Verizon Comments at 6 (“But to strike an appropriate balance, the Commission should also apply performance and validation standards to cell detection systems to ensure that termination of detected devices will not ensnare legitimate users that live or commute near correctional facilities.”).

verify the legitimacy of service termination requests, and that it should enact procedures to ensure that CISs continue to only capture accurate data after initial certification.<sup>20</sup>

**D. The Source of a Qualifying Request Should be Carefully Defined**

Finally, to ensure that a qualifying request is accurate, the source of the qualifying request – the Designated Correctional Facility Official (“DCFO”) should be carefully defined by the Commission. The Commission should define a DCFO to ensure that the party making and certifying the qualifying request is someone with the authority and incentive to verify the accuracy of any list of contraband devices.

Commenters agree that the DCFO must be carefully chosen, as this individual will need to perform several functions. First, the DCFO will need to be of a sufficiently high rank that he or she is in the position to oversee the CIS operator and validate the CIS’ findings. He or she also must be positioned to provide the various certifications that should be required to validate the request. Second, the DCFO will need to be familiar with the terms of any applicable leases between the CIS vendor and wireless carriers, and be in a position to affirm that the CIS is adhering to the parameters of its lease (in particular, that the signal is not bleeding outside the area governed by the spectrum lease and thus capturing authorized uses).<sup>21</sup> AT&T agrees that this person should be a state or local government official, as this will help promote accountability

---

<sup>20</sup> CTIA Comments at 5 (“Finally, the Commission should ensure that the provider of a certified and validated cell detection system regularly calibrates the system’s operations to ensure accuracy after initial device certification and solution validation. This will provide additional assurance that the data used as the basis for the request is accurate and reliable.”); T-Mobile Comments at 8-9 (“The Commission should maintain a list of certified CIS and CIS operators that can be used by the CMRS industry to verify the legitimacy of service termination requests.”).

<sup>21</sup> Verizon Comments at 5.

in the process.<sup>22</sup> And, finally, the DCFO must be carefully selected to ensure that the person making the termination request not only has the incentive to maintain its accuracy, but also lacks any incentive to compromise the qualifying request process.<sup>23</sup>

### **III. THE COMMISSION SHOULD NOT ADOPT A DEVICE DISABLING REQUIREMENT**

AT&T agrees with commenters who ask the Commission not to require wireless carriers to completely disable a device. At most, the Commission should require wireless carriers to terminate service to devices identified as contraband. The record demonstrates that complete disabling of a device as described by the Commission is not technically possible at this time. Second, even if device disabling did become technically feasible at a later date, it would be easy for inmates to circumvent. Third, the arguments in favor of complete device disabling suggest that a non-technical solution may be the remedy that best meets proponents' needs. Conversely, the termination of service is a capability available to all wireless carriers with respect to all devices, can be leveraged to meet the needs of the corrections community, and will be less harmful to lawful users.

---

<sup>22</sup> CTIA Comments at 6 (“If the Commission determines it cannot participate, then the only reasonable alternative is that all requests come from a senior state official with oversight of the CIS operator. The rules should not require wireless providers to respond to requests by non-sworn law enforcement officials, *e.g.*, a warden at a privately owned and operated correctional facility or from the CIS itself.”); Verizon Comments at 5 (“And DCFO requests should originate from those state or local government officials with oversight responsibility over the CIS provider vendor’s contract and operations. That will ensure accountability by the state or local officials directly responsible for the CIS provider’s acts and omissions.”).

<sup>23</sup> Cell Command Comments at 14 (“Third, there is still the chance that the person who smuggled the device into the facility is the same one that will be in charge of making the termination request, potentially reducing the likelihood that the termination request will ever be made.”).

In their opening comments, several parties observe that completely disabling all functions of a phone is technically infeasible at this time. As Verizon observes, the ability to fully and remotely disable (and re-enable) a handset by disabling or locking it entirely is currently limited to certain smartphone models, and is not available for feature phones or other connected devices.<sup>24</sup> Even on those devices where disabling is possible, device identifiers cannot be used to effectuate the disabling of the device – the capability is instead tied to the user’s account with their operating system provider (such as iOS or Android).<sup>25</sup> In other words, a disabling requirement would impact a fraction of contraband devices in prisons, and even then the *carrier* would not be able to independently effectuate the disabling without operating system provider involvement. As Verizon observes, “[t]o remotely and reliably disable appropriate devices would require extensive development by a number of players in the wireless ecosystem. And even once developed, the capability would not address the large embedded base of handsets in the marketplace today.”<sup>26</sup> Thus, not only would the process of developing disabling capability be a highly onerous one, but it would also have limited utility because the capability could only be adopted on a forward-looking basis.<sup>27</sup> For such capability to become ubiquitous, the current

---

<sup>24</sup> Verizon Comments at 9. *See also* Cell Command Comments at 14 (“Indeed, we are unaware of any technology being used by the carriers that would enable them to completely disable all functions and memory on a wireless device.”).

<sup>25</sup> Verizon Comments at 9.

<sup>26</sup> *Id.* at 8.

<sup>27</sup> *Id.* at 9.

embedded base of handsets would need to drop out of use – a years-long process.<sup>28</sup> And if this technology were to fall into the wrong hands, the results could be devastating.<sup>29</sup>

Because complete, remote device disabling by a wireless carrier is not achievable at this time, it is not an effective remedy to the contraband phones problem. Should the Commission adopt a requirement that this capability be provided by a certain future date, inmates simply will continue to use phones whose manufacture pre-dates the development of technology that renders devices inoperable. As stakeholders from the corrections community acknowledge, inmates are generally aware of which devices are easiest to use – and conceal – illicitly, and have adjusted their behavior accordingly.<sup>30</sup> Furthermore, given that inmates lack freedom of movement and are not able to walk into a store and upgrade their device, it is likely that the pool of devices used illicitly in correctional facilities, in general, will employ older technology than the pool of devices in the general population. For this reason, any solution that relies on advanced device

---

<sup>28</sup> *Id.* at 10 (“Finally, once the new capability could be available, it still would take years for the embedded base of handsets to drop out of use before this capability could have a meaningful impact. The Commission’s and industry’s experience in transitioning the embedded base of handsets to E-911 location-capable models illustrates how handset turnover can resist carrier marketing efforts.”).

<sup>29</sup> CTIA Comments at 7 (“This approach, however, requires broader stakeholder input, including participation by the original equipment manufacturers (‘OEMs’), and it creates other risks including expanded cybersecurity threats as a ‘shut down’ mechanism would be available to hackers.”).

<sup>30</sup> *See, e.g.*, Comments of the Tennessee Department of Correction, GN Docket No. 13-111, at 4 (June 19, 2017) (“TDOC Comments”) (“Further exacerbating the problem, inmates have begun using small Bluetooth devices to make calls over connected-but-remotely-hidden contraband cellphones. As a result, correctional facility employees are forced to attempt to locate ever-smaller adjunct devices being used by inmates for illegal communications, as well as the connected contraband cellphones that may be hidden at another location entirely.”).

capabilities only available on as-yet-undeveloped hardware is unlikely to be effective in the near term, if at all.

Based on the comments filed by corrections stakeholders in this proceeding, it appears that the most effective “device disabling” solution may be a non-technical one. Corrections commenters have expressed a desire that *all* functions of a contraband phone be disabled, including those not requiring wireless connectivity and including those that are not unique to cell phones.<sup>31</sup> To that end, the solution that best meets the stated needs of corrections is physical confiscation of the phone.<sup>32</sup> As explained further below, not even jammers would achieve the outcome desired by corrections officials. Thus, AT&T echoes Commissioner O’Rielly’s calls for the examination of non-technical solutions that result in either the confiscation of contraband devices and/or the prevention of device smuggling.<sup>33</sup>

---

<sup>31</sup> See, e.g., Letter from Lannette C. Linthicum and James A. Gondles, Jr., American Correctional Association to Marlene H. Dortch, Federal Communications Commission, GN Docket No. 13-111, at 2 (“ACA Comments”) (“The technology must be able to completely render the wireless device unusable, with the possible exception of 9-1-1, preventing all other voice calls, data usage, memory function, photography or any other function or application that can be used to transmit or record any form of communications, even by passing the device physically.”).

<sup>32</sup> While law enforcement functions related to the possession of contraband obviously is outside the scope of the Commission’s jurisdiction, AT&T notes commenters’ calls for more aggressive search and seizure of contraband, including efforts aimed at preventing corrections staff from bringing in contraband.

<sup>33</sup> *Further Notice* at Statement of Commissioner Michael O’Rielly (“O’Rielly Statement”) (“It seems like these systems are expensive and that there are alternatives, such as metal detectors, that are cheaper and potentially more effective at detecting all contraband, including cellphones.”). See also, e.g., Letter from Paul Wright, Human Rights Defense Center to Ajit Pai, Chairman, Federal Communications Commission, GN Docket No. 13-111, at 6 (June 19, 2017) (“HRDC Comments”) (“A technological solution will not be effective until the supply chain is cut off.”).

For the foregoing reasons, if the Commission adopts its proposed “qualifying request” mechanism, wireless carriers should be directed only to terminate service to an identified contraband device, not disable the device entirely. Not only is service termination technically feasible vis-à-vis all service-initialized devices (including feature phones and legacy devices), but it also is an established, common practice for wireless carriers and their customers. Indeed, “wireless providers can adapt their existing fraud prevention and law enforcement support systems to process service termination requests without the need to also develop and deploy the new device or network capabilities needed to completely disable the device.”<sup>34</sup> Wireless carriers already have personnel who are trained to deal with termination of service matters, and implementation of a service termination requirement is much simpler than a device disabling requirement. In the event a law-abiding user is wrongfully included in a qualifying request, their injury will be less severe if service is merely terminated to their device, as opposed to their device being rendered unusable (and stored content potentially being lost). And although corrections commenters cite the problem of SIM card swapping in support of technologies that disable devices,<sup>35</sup> CTIA notes that by continuously sweeping their facilities, correctional institutions can make it much more difficult for inmates to engage in this practice.<sup>36</sup> For these

---

<sup>34</sup> Verizon Comments at 8-9.

<sup>35</sup> See, e.g., Comments of Global Tel\*Link Corporation, GN Docket No. 13-111, at 5 (June 19, 2017) (“GTL Comments”).

<sup>36</sup> CTIA Comments at 7 (“A fully effective and engaged [cell detection system] will allow correctional institutions to continuously or regularly sweep their facilities – rather than merely capturing IMSI use at a single point in time – so that the attempted use of swapped out SIMs in a single device will result in the identification of multiple unauthorized IMSIs, making it much more difficult for inmates to use contraband wireless devices.”).



reasons, a service termination requirement is much more consistent with technical realities and the policy goals of this proceeding than a device disabling requirement.

#### **IV. ANY TECHNICAL SOLUTION MUST BE TECHNOLOGY NEUTRAL AND NOT HARM WIRELESS NETWORKS OR USERS**

##### **A. Proposals to Require Beaconing Technology Violate Principles of Technological Neutrality**

One potential solution raised by the Commission and advocated by commenters is the use of beacon-based solutions in prisons to remotely disable contraband phones. As explained further below, these solutions cannot be implemented without a Commission mandate that certain software be installed on wireless handsets. Not only do carriers have limited ability to control the design of wireless equipment, but such a proposal clearly violates the Commission's longstanding policy of technological neutrality. Furthermore, these technologies would be ineffective if a contraband device does not contain the required software. And, finally, a beacon mandate could lead to the use of beacons without the knowledge or consent of consumers in contexts that go well beyond prisons, creating enormous problems for consumers.

Beacon-based solutions clearly violate the Commission's policy of technical neutrality because for beacons to be effective, the Commission must mandate aspects of handset design. Cell Command, the primary proponent of beacons in this proceeding, explains that hardware installed by prisons will interact with software contained on contraband phones to essentially "brick" the device.<sup>37</sup> As Cell Command admits in its comments, its system will not be effective unless the Commission mandates the inclusion of Cell Command's software on all mobile

---

<sup>37</sup> Cell Command Comments at 4.

handsets in the United States.<sup>38</sup> Advocates of beacon technologies presume that wireless carriers design or have the ability to control the design of handsets – they do not. Further, as T-Mobile observes, “[r]ules that effectively promote the deployment of a particular technology would be inconsistent with the Commission’s policy against choosing technological winners and losers.”<sup>39</sup>

In addition, a beacon mandate suffers from the same flaws as a device disabling mandate – it will take time to implement, is not backwards-compatible with all handsets currently in use, and thus would not have any near-term benefits.<sup>40</sup> As Verizon explains, “[b]eacon-based solutions are dependent not only on the capabilities of devices and the ability of OEMs to integrate the relevant hardware and software capabilities into their products, but the ubiquity of capable devices (and absence of non-capable devices) among users, and the ubiquitous deployment of beacon devices throughout a correctional facility.”<sup>41</sup> This ubiquity cannot be

---

<sup>38</sup> *Id.* at 16.

<sup>39</sup> T-Mobile Comments at 15. *See also* CTIA Comments at 9-10 (“First, implementation of these systems would require all existing and future wireless devices to include the software. As recognized by Commissioner O’Rielly, this would be a dramatic departure from the Commission’s long-standing policy to remain technology-neutral and it would involve a sweeping government mandate.”) (footnotes omitted).

<sup>40</sup> In addition, CTIA highlights the potential cybersecurity threat posed by beacons. CTIA Comments at 10 (“Further, it would be ineffective, burdensome, and costly, with a lengthy implementation process. It also would pose a cybersecurity threat to public safety by introducing a nationwide capability that could be used to block legitimate calls.”).

<sup>41</sup> Verizon Comments at 13. *See also* Cell Command Comments at 5 (“In order to be effective, the solution must be ubiquitous and work on *all* wireless devices. If it does not, inmates and their co-conspirators will identify the devices that will still work, and use those devices to continue criminal business as usual.”).

achieved any time soon,<sup>42</sup> and in its absence inmates simply will continue to use phones that do not contain the beacon software. Even if the Commission mandated support for beaconing systems in the U.S., it could not control the importation of wireless devices from overseas that are smuggled into prisons with the intent of evading the beacon.<sup>43</sup>

Furthermore, if the Commission were to require the installation of beacon software on all phones, there would be no way to prevent misuse of beacon technologies in other contexts. Cell Command does not indicate that it would limit licensing of its technology to prisons, instead simply stating that it is willing to license its technology “to device and beacon manufacturers on fair, reasonable and non-discriminatory terms.”<sup>44</sup> The Commission’s enforcement actions related to jammers demonstrate that corrections officials are far from the only people who wish to block individuals’ wireless capability without their consent.<sup>45</sup> AT&T shares T-Mobile’s concern that if the Commission were to mandate beacon compatibility on all phones, the result would be

---

<sup>42</sup> The American Correctional Association appears to concede this point, asking the Commission and wireless industry to agree to a two-year phase-in period for beacon technologies. ACA Comments at 4.

<sup>43</sup> See T-Mobile Comments at 19 (“Finally, the TSF solution will not cure the contraband phone problem. It would merely encourage the use of phones without the TSF software. If the FCC requires all handsets operating or manufactured for sale in the U.S. to have the necessary software, a cottage industry will be created where handsets manufactured for sale overseas are smuggled into prisons.”).

<sup>44</sup> Cell Command Comments at 3.

<sup>45</sup> See, e.g., Chris Matyszczyk, *FCC: Man used device to jam drivers’ cell phone calls*, CNET.COM (May 1, 2014), at <https://www.cnet.com/news/man-put-cell-phone-jammer-in-car-to-stop-driver-calls-fcc-says/> (describes FCC enforcement action against a man who used a jammer in his car because he appeared to be “frustrated with people making cell phone calls in their cars”). See also Chris Matyszczyk, *Science teacher suspended for using jammer to shut up students’ cell phones*, CNET.com (June 3, 2015), at <https://www.cnet.com/news/science-teacher-suspended-for-using-jammer-to-shut-up-students-cell-phones/> (describing the case of a teacher who installed a cell phone jammer in his classroom).

“mission creep”<sup>46</sup> – with other institutions installing beacons without the knowledge of the public. Such an outcome is clearly contrary to the public interest.

A beacon is, in the strictest sense, a simple transmitter that emits a continuous signal. Under the use case proposed by Cell Command, a beacon would force a cell phone to transmit a signal, which would enable corrections officials to track down the phone.<sup>47</sup> AT&T notes that the handheld Stingray devices already used by law enforcement work in essentially the same way, and thus law enforcement already has access to technology that could accomplish the same functionality as a beacon system. While the use of these devices has been controversial, the sorts of privacy concerns raised in connection with their use outside of prison walls would not be present in the prison context. In other words, law enforcement could achieve similar functionality without the need for the Commission to impose a technological mandate that runs counter to its principles of technological neutrality.

**B. Mandated Quiet Zones Would Frustrate Network Design and Degrade Service Quality Near Correctional Facilities**

AT&T also opposes calls for wireless carriers to create “quiet zones” in the areas surrounding correctional facilities. In discussing this proposal in the *Further Notice*, the Commission explains that “the common goal seems to be the creation of areas in which communications are not authorized such that contraband wireless devices in correctional

---

<sup>46</sup> T-Mobile Comments at 18 (“It would also create the risks of privacy, security, and ‘mission creep’ – terminating service to phones in contexts outside the clearly warranted case of contraband devices – noted above with respect to any mandated software changes to enable remote service termination by a party other than the authorized owner.”).

<sup>47</sup> Cell Command Comments at 17.

facilities would not receive service from a wireless provider.”<sup>48</sup> AT&T joins commenters who oppose any sort of “quiet zone” mandate, as this solution is technologically unworkable, would negatively and unfairly impact lawful users, and would unduly interfere with wireless providers’ ability to design their networks.

“Quiet zone” proposals are based on the premise that wireless carriers could retrofit their networks to carve out coverage of correctional facilities – and *only* correctional facilities. This simply is not technically possible and is “based on a flawed understanding of RF propagation.”<sup>49</sup> As CTIA explains, “a quiet zone network design cannot stop at a barbed wire fence.”<sup>50</sup> As commenters observe, the only way for a carrier to carve out the entirety of a correctional facility from coverage is to eliminate coverage from a much larger area surrounding the prison.<sup>51</sup> In other words, carriers could not create “quiet zones” within prisons without denying service to lawful users inside the facility, as well as those who live nearby or who are traveling in the general vicinity of a correctional facility.<sup>52</sup> Such an action plainly does not serve the public interest.

---

<sup>48</sup> *Further Notice* at ¶ 123.

<sup>49</sup> Letter from J3 Technologies LLC to Marlene H. Dortch, Federal Communications Commission, GN Docket No. 13-111, at 1-2 (filed June 23, 2017).

<sup>50</sup> CTIA Comments at 10.

<sup>51</sup> T-Mobile Comments at 16 (“Given the propagation characteristics of radio frequencies, it is impossible to carve out the specific boundaries of a correctional facility from coverage. To create a ‘quiet zone’ around such facilities, carriers would have to eliminate coverage to a much larger area surrounding the facility to ensure no radio signals reach the correctional facility.”).

<sup>52</sup> CTIA Comments at 10 (“FCC-imposed quiet zones around correctional facilities would have the effect of preventing legitimate communications, including public safety communications on commercial networks, on prison grounds and beyond.”); T-Mobile

While the proposed quiet zone requirement has the potential to negatively impact wireless users in a variety of areas, perhaps no group will be placed more at risk than those in rural areas. To cover rural areas, wireless carriers typically use higher power antennas on taller towers, so that they can cover greater distances with a single cell site.<sup>53</sup> It would be extremely costly to carriers to require them to re-design their networks to accommodate prisons – something that was not envisioned when they acquired their licenses, either at auction or on the secondary market. Many correctional facilities are located in rural areas, and out of necessity a rural “quiet zone” may need to cover more non-prison territory than an urban “quiet zone,”<sup>54</sup> thus injuring law-abiding rural subscribers.

Even if the creation of “perfect” quiet zones was possible – which it is not – a requirement to create these quiet zones would place an enormous burden on wireless carriers and promote inefficient network design. Wireless carriers would be required to re-design their networks and/or power down their base stations to create the quiet zone.<sup>55</sup> Because wireless

---

Comments at 16 (“Such actions would prevent individuals and families living in, working in, or passing through the vicinity of a correctional facility from obtaining reliable wireless service.”).

<sup>53</sup> See CTIA Comments at 10-11 (“Further, in rural areas, wireless service often is provided via higher power antennas on taller towers that cover great distances, and a network re-design to engineer quiet zones could easily take rural consumers near correctional facilities out of service.”).

<sup>54</sup> AT&T stresses, however, that subscribers in urban areas near correctional facilities would also be impacted, and as a general matter correctional facilities are not as remote as commenters in this proceeding have described them. CTIA Comments at 11 (“Even in urban areas, quiet zones would have to extend substantially beyond the bounds of the prison property. And because some correctional facilities are located near busy interstates and well-traveled state routes, and are not ‘relatively remote’ as other parties have suggested, quiet zones could take travelers out of service.”).

<sup>55</sup> Verizon Comments at 12 (“The construction of new correctional facilities, or an existing correctional facility’s authorization for new quiet zone status within licensees’ existing coverage

networks have been designed to maximize coverage both indoors and outdoors, and to make the most efficient use of base stations, retrofitting already-deployed networks to create quiet zones would be an extremely complicated endeavor.<sup>56</sup> Further, it would impose significant costs on licensees and would implicate Section 316 of the Communications Act by modifying a wireless provider's geographic area license without an adjudication.<sup>57</sup>

**C. Jamming Technology is Prohibited by the Communications Act, Harmful to Lawful Wireless Users, and Counterproductive**

Notwithstanding the fact that jammers are illegal in the United States, some commenters continue to call for the Commission to authorize the use of jamming technologies in correctional facilities.<sup>58</sup> Not only are jammers illegal, but they also have the potential to greatly harm

---

areas, would require that wireless providers either re-design their radio access networks or substantially power down their transmitters.”).

<sup>56</sup> T-Mobile Comments at 16 (“CMRS systems are designed to maximize coverage within the geographic area covered by the license. Radio and antenna systems are designed to maximize coverage both outdoors and indoors, which requires a stronger signal to account for building losses. To design a network to avoid coverage to a specific portion of the licensed area is inapposite to long-standing network design concepts.”).

<sup>57</sup> See Verizon Comments at 12 (“Both options would impose significant costs on licensees and adversely affect the reliability of service to consumers. Many correctional facilities are in or near urban and suburban areas and major thoroughfares with established coverage and that are the focus of licensees’ ongoing network densification and 5G deployment efforts. This approach would also implicate Section 316 of the Act by modifying a wireless provider’s licensed geographic area without an adjudication.”).

<sup>58</sup> Letter from Leann Bertsch, President of The Association of State Correctional Administrators, to Marlene H. Dortch, Federal Communications Commission, GN Docket No. 13-111, at 1 (June 19, 2017) (“I am writing today to ask that you amend your proposed rule to include surgical jamming technology, and to provide measures to ensure carrier cooperation with beacon technology, managed access technology and future technologies.”); GTL Comments at 8 (“GTL supports the use of jamming technologies when appropriate for a particular correctional facility setting.”); TDOC Comments at 1 (“The TDOC asks the Commission to amend the proposed rule to authorize the development of jamming technology and to provide stringent measures to ensure carrier cooperation with future technologies.”).

authorized users, are prone to manipulation, and would not meet the stated objectives of the corrections community. Thus, jammers would be an inappropriate solution to the problem of contraband phones in prisons.

The stakeholders in this proceeding – including the Commission – have made clear on numerous occasions that jamming technology is illegal. In fact, the illegality of jammers is well-established. In the initial *Notice of Proposed Rulemaking* in this proceeding, the Commission reiterated the fact that the Communications Act prohibits both the operation of a jammer as well as the manufacture, importation, marketing, and sale of jammers in the United States.<sup>59</sup> In recent years, the Commission has aggressively enforced the prohibition on jammers, issuing enforcement advisories in multiple languages and taking enforcement actions against numerous violators.<sup>60</sup> In his statement on the *Further Notice*, Commissioner O’Rielly pledged never to support or approve of any form of jamming technologies in this proceeding.<sup>61</sup>

---

<sup>59</sup> *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, et al.*, Notice of Proposed Rulemaking, 28 FCC Rcd 6603, ¶ 19 (2013) (“The Act prohibits any person from willfully or maliciously interfering with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government. Because radio signal jammers are used to willfully interfere with radio communications of such licensed or authorized stations, jammers are not permitted under the Commission’s rules. Similarly, the manufacture, importation, marketing, sale, or operation of radio signal jamming devices within the United States is prohibited, except for the sale to or use by the Federal Government.”).

<sup>60</sup> Federal Communications Commission, Jammer enforcement, at <https://www.fcc.gov/general/jammer-enforcement> (last visited July 17, 2017).

<sup>61</sup> See O’Rielly Statement (“Lastly, I do want to make one position crystal clear: no matter how this proceeding moves forward, I will not support or approve of any form of jamming technologies.”).



Even if the Commission were to permit jamming only in the limited context of curbing contraband phone use in correctional facilities, it would greatly frustrate the Commission's enforcement efforts in other areas. As of March 2017, there were 1,719 state prisons in the U.S., as well as thousands of juvenile correctional facilities and local jails.<sup>62</sup> If the Commission allowed jamming in the context of these facilities, the sheer number of jammers sold and/or imported in the United States would inevitably frustrate any continued Federal prohibition on jamming in other contexts. By increasing the number of jammers present in the U.S. legally, the number of illegal jammers would no doubt increase as well, greatly increasing the Commission's enforcement burden.

In addition to being illegal, jammers have the potential to greatly harm authorized users of wireless services both inside and outside of corrections facilities. For a jammer to be effective its signal will need to cover every inch of a prison accessible by inmates. If it does not, inmates will find and exploit the jammer's weaknesses. As was the case for "quiet zones," to ensure every inch of a correctional facility is covered, a jammer necessarily would have to over-jam and have its signal bleed outside of a corrections facility. As the American Correctional Association concedes, jamming technologies "interfere with communications signals outside the correctional facility."<sup>63</sup> Not only would wireless users in the vicinity of a correctional facility be put at risk,

---

<sup>62</sup> See Peter Wagner and Bernadette Rabuy, "Mass Incarceration: The Whole Pie 2017," Prison Policy Initiative (March 14, 2017), at <https://www.prisonpolicy.org/reports/pie2017.html>.

<sup>63</sup> ACA Comments at 2. See also Cell Command Comments at 11 ("Second, jamming and geo-fencing also have the real potential to interfere with legitimate wireless devices operating within the range of the jamming system.").

but jammers also would interfere with emergency personnel responding to an emergency inside a correctional facility, or other authorized uses that may be allowed within a particular facility.

Jammers are also an inappropriate solution because they are prone to manipulation and circumvention. Numerous prisons outside of the United States have deployed jammers as a means of dealing with contraband cell phones. These efforts demonstrate the limits of jamming technology and the challenges associated with policing unauthorized uses. Enterprising inmates have found ways to circumvent jammers installed in overseas prisons. In India, prisoners searched for areas within the prison not covered by the jammer, then strung earphones to that location to achieve mobile connectivity.<sup>64</sup> In Ireland, inmates foiled jammers by using Skype and satellite phones to bypass jamming technology.<sup>65</sup> In some cases, prison employees have been complicit in compromising a jammer. In the Bahamas, a prison guard faced trial for allowing three inmates to damage a jammer, rendering it inoperable and enabling unauthorized wireless use by inmates.<sup>66</sup> At one prison in the Philippines, prison officials accepted bribes in exchange for keeping cell jammers turned off most of the time.<sup>67</sup> In other words, just one

---

<sup>64</sup> Chetan R., *Tech-Savvy Jailbirds Bypass Jammers*, BANGALORE MIRROR (Mar. 25, 2014), available at <http://bangaloremirror.indiatimes.com/bangalore/crime/central-jail-brass-jailbirds-neutralised-earphones-parappana-agrahara-central-prisons-jammer/articleshow/32614735.cms?>.

<sup>65</sup> Cormac O’Keeffe, *Inmates foil mobile phone blockers*, IRISH EXAMINER (Dec. 29, 2009), available at <http://www.irishexaminer.com/ireland/icrime/inmates-foil-mobile-phone-blockers-108631.html>.

<sup>66</sup> Artesia Davis, *Prison guard on trial in connection with cell phone jammer damage*, THE NASSAU GUARDIAN (Feb. 13, 2016), available at <http://www.thenassauguardian.com/news/62685-prison-guard-on-trial-in-connection-with-cell-phone-jammer-damage>.

<sup>67</sup> Delon Porcalla, *Lifestyles of the prison’s rich and famous*, THE PHILIPPINE STAR (Oct. 11, 2016), available at <http://www.philstar.com/headlines/2016/10/11/1632458/lifestyles-prisons-rich-and-infamous>.

enterprising inmate or rogue prison employee can render a jammer completely useless; thus jammers are not the panacea that some stakeholders in this proceeding hope they can be.

## **V. CONCLUSION**

Key stakeholders in this proceeding agree that any processes adopted to combat contraband phone use be efficient, accurately capture unlawful uses, and protect lawful users. As the Commission considers rules in this proceeding, it should only adopt those rules that are technically feasible, consistent with policies of technical neutrality, and unlikely to harm wireless networks. By acting consistent with the policies articulated herein, the Commission will make great strides in addressing the problem of contraband phones in correctional facilities.

Respectfully Submitted,

/s/ Jessica B. Lyons

---

Jessica B. Lyons  
Michael P. Goggin  
Gary L. Phillips  
David L. Lawson  
AT&T Services, Inc.  
1120 20<sup>th</sup> Street, N.W.  
Washington, D.C. 20036  
202-457-2100  
*Its Attorneys*

July 17, 2017