

**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 INPIXON USA**

Steven A. Augustino  
Ross G. Slutsky  
Kelley Drye & Warren LLP  
3050 K Street, NW  
Suite 400  
Washington, D.C. 20007-5108  
(202) 342-8612

*Counsel to Inpixon USA*

July 17, 2017

## TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION AND SUMMARY .....</b>	<b>1</b>
<b>II.</b>	<b>THE COMMISSION SHOULD ADOPT AN INCLUSIVE AND TECHNOLOGICALLY NEUTRAL DEFINITION OF CONTRABAND INTERDICTION SYSTEMS .....</b>	<b>2</b>
<b>III.</b>	<b>THE COMMISSION SHOULD REJECT CELL COMMAND’S ANTI-COMPETITIVE PROPOSAL FOR A BEACON MANDATE .....</b>	<b>4</b>
A.	Cell Command’s Beacon Mandate Would Not Effectively Achieve the Commission’s Public Safety Objectives.....	5
1.	Beacon efficacy relies on conditions that would be unrealistic on a national scale .....	5
2.	Even if the Commission mandated beacons, the software would remain vulnerable to hacking .....	7
B.	Cell Command’s Beacon Mandate Would Be Prohibitively Expensive .....	7
C.	Cell Command’s Beacon Mandate is Anti-Competitive .....	9
<b>IV.</b>	<b>CONCLUSION .....</b>	<b>11</b>

**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 INPIXON USA**

**I. INTRODUCTION AND SUMMARY**

Inpixon USA (“Inpixon” or “Company”) respectfully submits these reply comments in response to the Federal Communications Commission’s (“FCC” or “Commission”) *Report & Order and Further Notice of Proposed Rulemaking (“FNPRM”)* in the above-captioned proceeding.

Inpixon generally supports the FCC’s efforts to improve the contraband wireless device interdiction process. The procedural rule changes proposed by the Commission are an important step in the right direction. However, there are two particular matters that the Company would like to draw attention to: (1) the FCC should revise the definition of a Contraband Interdiction System (“CIS”) to include fully passive detection systems; and (2) should reject Cell Command’s anti-competitive request for a beacon mandate.

Under its current formulation, the definition of a CIS requires the inclusion of a transmission capability. Such a requirement has the secondary effect of excluding fully passive detection systems, despite the fact that “detect and locate” systems are vital to the interdiction process, are widely utilized in correctional facilities, and would otherwise satisfy the Commission’s proposed CIS eligibility requirements. Accordingly, Inpixon urges the Commission to revise the definition of a CIS (at 47 C.F.R. § 1.9003) to read as follows:

- *Contraband Interdiction System.* Contraband Interdiction System is a system that **detects and/or** transmits communication signals comprised of one or more stations used only in a correctional facility exclusively to prevent transmissions to or from contraband wireless devices within the boundaries of the facility and/or to obtain identifying information from such contraband wireless devices.

Inpixon joins numerous industry voices on the record in this proceeding in urging the FCC to refrain from imposing a federal beacon mandate, and instead maintain its longstanding policy of technological neutrality. Although Cell Command has claimed that it merely seeks for the Commission to create a voluntary process for industry to adopt its beacon software, its initial comments strongly suggest a preference for a mandate, and, in any event, urge agency action that would place the Commission in the inappropriate position of favoring one technological solution over another. While beacons may be useful in some environments, they are subject to numerous scaling and security constraints that make it inappropriate to mandate at the national level. Inpixon and a variety of industry commenters believe that a beacon mandate would also prove prohibitively expensive. Finally, Inpixon urges the Commission to reject Cell Command's beacon mandate on the grounds that it is anti-competitive and detrimental to public safety insofar as it would lock in a particular solution regardless of the actual needs of any given facility.

## **II. THE COMMISSION SHOULD ADOPT AN INCLUSIVE AND TECHNOLOGICALLY NEUTRAL DEFINITION OF CONTRABAND INTERDICTION SYSTEMS**

Inpixon recommends that the FCC revise the definition of a Contraband Interdiction System ("CIS") in a manner that includes fully passive (i.e. real-time trilateration) detection systems. In the Report & Order preceding the *FNPRM*, the Commission defined a CIS as a "system that transmits radio communication signals comprised of one or more stations used only in a correctional facility exclusively to prevent transmissions to or from contraband wireless devices within the boundaries of the facility and/or to obtain identifying information from such

contraband wireless devices.”<sup>1</sup> To better reflect the scope and nature of interdiction solutions in the marketplace, the Commission should revise this definition to state that a “system that *detects and/or* transmits radio communication signals” qualifies as a CIS.

The Commission should take action to ensure that the definition of a CIS is technologically neutral. By requiring that CIS solutions include direct transmission capabilities, the Commission skewed the class of eligible services in the direction of Managed Access Systems (“MAS”) while excluding a broad array of detection and location services that just as effectively identify contraband communications and enable correctional facilities to act on such information. As several parties to this proceeding have observed, correctional facilities range from “municipal and county jails housing fewer than ten inmates” to “state and federal maximum-security systems housing tens of thousands of inmates.”<sup>2</sup> While MAS solutions can be useful for certain facilities, as the American Correctional Association (“ACA”) observed, “MAS is not fool-proof and is far too expensive for most correctional facilities.”<sup>3</sup> Inpixon is confident that its Indoor Positioning Analytics (“IPA”) solution compares favorably to MAS solutions on numerous price and performance metrics.

Detection is an essential element of any interdiction tool and deserves inclusion in the CIS category whether detection is performed through active transmissions or passive systems like Inpixon’s IPA solution. Inpixon IPA meets all of the FCC’s proposed location accuracy, information quality, and data security standards and would otherwise qualify as an eligible CIS.<sup>4</sup>

---

<sup>1</sup> *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd at 2387 (2017) (“*FNPRM*”).

<sup>2</sup> *Id.*

<sup>3</sup> ACA *FNPRM* Comments at 2. *See also* Prelude Communications *FNPRM* Comments at 5-6.

<sup>4</sup> *See FNPRM*, 32 FCC Rcd at 2393.

While the Commission correctly observed in the *FNPRM* that passive detection systems inherently do not require FCC authorization for spectrum licenses,<sup>5</sup> Inpixon is concerned about unintended consequences of the present definition of a CIS. If the Commission grants correctional officers the ability to direct wireless carriers to disable specific devices identified via a CIS, then equally effective passive detection systems should be included in the definition of a CIS. In addition, Inpixon is concerned that correctional facility Requests for Proposal (“RFPs”) may start mandating the use of CIS meeting the FCC’s definition, thereby inadvertently excluding sophisticated passive solutions that are equally or better suited to the needs of such facilities but would not (absent the change Inpixon recommends) meet the technical definition of a CIS. Accordingly, Inpixon requests that the Commission modify the definition of a CIS to include passive detection systems.

### **III. THE COMMISSION SHOULD REJECT CELL COMMAND’S ANTI-COMPETITIVE PROPOSAL FOR A BEACON MANDATE**

In its comments, Cell Command took the somewhat unusual approach of requesting that the FCC intervene on its behalf to mandate the use of its technology. While Cell Command may dispute such a characterization of its intentions, for reasons discussed below, Cell Command’s desire for a beacon mandate is abundantly clear.<sup>6</sup> Echoing the shared sentiments of numerous industry stakeholders in this proceeding,<sup>7</sup> Inpixon opposes Cell

---

<sup>5</sup> *FNPRM*, at ¶ 79.

<sup>6</sup> *See infra*, Part III(C).

<sup>7</sup> *See, e.g.*, CTIA *FNPRM* Comments at 9 (“The Commission should refrain from dictating use of a beacon system”); T-Mobile *FNPRM* Comments at 18 (“The Commission should not mandate the use of proprietary beacon technology”); Verizon *FNPRM* Comments at 113 (“[beacons and similar technologies] would ... take years to implement and even longer to meaningfully limit the abuse of contraband handsets.”); Global Tel\* Link *FNPRM* Comments at 2 (“GTL’s experience demonstrates that mandating a one-size-fits-all technical solution is not workable”).

Command's request on three primary grounds: a beacon mandate would be ineffective, costly, and anti-competitive.

**A. Cell Command's Beacon Mandate Would Not Effectively Achieve the Commission's Public Safety Objectives**

While beacon technologies may be suitable for particular facilities and circumstances, they are not a panacea, and, accordingly, should not be treated as one. As Inpixon explains below, beacon technologies rely on conditions that would be difficult or impossible to realize on a national scale, and could ironically pose new threats to security and public safety if mandated on a national scale.

**1. Beacon efficacy relies on conditions that would be unrealistic on a national scale**

As Cell Command itself recognized, its solution only works if numerous conditions are in place. Cell Command acknowledges at the outset that its solution requires that "software is embedded ... into the firmware of all cell phones."<sup>8</sup> Carriers have consistently questioned the feasibility of such universal implementation. For example, Verizon observed, "[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>9</sup>

Inpixon shares the carriers' skepticism about the feasibility of enabling every wireless device in the U.S. with beacon software. As of 2016, there were nearly 338 million cell

---

<sup>8</sup> Cell Command *FNPRM* Comments at 2 (emphasis added).

<sup>9</sup> Verizon *FNPRM* Comments at 13. *See also* CTIA *FNPRM* Comments at 9-10 "[I]mplementation of these systems would require all existing and future wireless devices to include the software."

phones in use in the United States.<sup>10</sup> Despite the prolonged growth and cultural impact of smart phones, Americans still rely on a variety of mobile cellular solutions and feature phones. From a technical perspective, it is not clear whether or how a carrier could push the beacon software update to a feature phone. Moreover, as Inpixon has previously emphasized, the issue of contraband communications in correctional facilities is not limited to cellular telephones.<sup>11</sup>

However, even if we were to assume that the Commission could impose a mandate on equipment manufacturers and/or carriers to retroactively push beacon software on all active wireless devices in the United States, beacon technology would still face serious challenges. As T-Mobile correctly observed, “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>12</sup> Furthermore, within the confines of the United States, a beacon mandate may result in a black market for people building their own devices or even configuring their own local area cellular networks to circumvent the beacon software.<sup>13</sup> Hence, in the face of imported devices and obvious black market incentives, forcing beacon technology on a national scale would prove imprudent.

---

<sup>10</sup> FCC, *Voice Telephone Services: Status as of June 30, 2016* (WCB 2017), available at: [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-344500A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DOC-344500A1.pdf), 10.

<sup>11</sup> Inpixon *FNPRM* Comments at 5-6.

<sup>12</sup> T-Mobile *FNPRM* Comments at 19.

<sup>13</sup> See Aaron Soupporis, *Build your own Cell Phone for \$200*, THE VERGE (November 28, 2013), available at <https://www.theverge.com/2013/11/28/5154536/how-to-build-your-own-cellphone-mit-media-lab-david-mellis>; Alex Cranz, *It Only Costs \$400 to Build Your Own Cell Phone Network*, GIZMODO (January 17, 2017), available at <https://gizmodo.com/it-only-costs-400-to-build-your-own-cell-phone-network-1791282980> (explaining a DIY project to create a software-defined radio to create a local network).



**2. Even if the Commission mandated beacons, the software would remain vulnerable to hacking**

In its effort to combat the use of contraband wireless devices, the Commission must remain focused on eliminating security risks without creating new ones. As T-Mobile observed, “[Cell Command’s proposed mandate] would also create... risks of privacy, security, and ‘mission creep’ – terminating service to phones in contexts outside the clearly warranted case of contraband devices.”<sup>14</sup> Similarly, CTIA acknowledged that a beacon mandate “would pose a cybersecurity threat to public safety by introducing a nationwide capability that could be used to block legitimate calls.”<sup>15</sup> Inpixon shares CTIA’s views on such matters, but believes that they might have understated the degree of the threat. Cell Command prides itself on the ability to “brick” contraband cellular devices by completely disabling them. Beyond merely call blocking, universalizing the ability to disable communications on all U.S. wireless devices could wreak havoc if such capabilities were to fall into the wrong hands. By nature, there is no such thing as perfect security. Theoretically, any company offering solutions in this industry could end up compromised. However, no other company in this proceeding seeks to force software onto every known wireless device in the United States and its territories. Accordingly, in weighing the costs and benefits of Cell Command’s proposal, the Commission should take into account the risk of a universal solution turning into a universal problem.

**B. Cell Command’s Beacon Mandate Would Be Prohibitively Expensive**

The Commission must recognize that implementing a beacon mandate could prove unaffordable for industry participants and correctional facilities alike. As Global Tel Link Communications correctly observed, the Commission needs to take into account budgetary

---

<sup>14</sup> T-Mobile *FNPRM* Comments at 18.

<sup>15</sup> CTIA *FNPRM* Comments at 9.

constraints when assessing the feasibility of various technological solutions.<sup>16</sup> Inpixon shares CTIA's view that a beacon mandate would be "ineffective, burdensome, and costly, with a lengthy implementation process."<sup>17</sup> Despite Cell Command's apparent interest in licensing out their solutions on fair, reasonable, and non-discriminatory ("FRAND") terms,<sup>18</sup> such an offering does not fully encapsulate the costs of the beacon mandate. Cell Command itself admits that it will not actually build the component parts of its system, which leaves separate developmental and manufacturing costs unaccounted for.<sup>19</sup>

Additionally, the FCC must take into account the considerable costs of equipment manufacturer and carrier beacon software integration. As ShawnTech Communications astutely observed, there is little or no information in the record concerning whether or how equipment manufacturers would absorb the costs of incorporating beacon software into their technologies.<sup>20</sup> Alternatively, if, as Cell Command suggests, the mandate were imposed on wireless carriers to push out software updates,<sup>21</sup> the scope of the mandate would only cover those devices that operate in relation to a carrier, neglecting the range of non-carrier frequencies and communications options available to enterprising inmates.<sup>22</sup> Under such a mandate, there would be additional costs to deal with the non-CMRS communications. Hence, in many respects, the costs of a beacon mandate appear to be considerable.

---

<sup>16</sup> See Global Tel Link Communications *FNPRM* Comments at 2.

<sup>17</sup> CTIA *FNPRM* Comments at 10.

<sup>18</sup> Cell Command *FNPRM* Comments at 18.

<sup>19</sup> *Id.*

<sup>20</sup> See ShawnTech Communications *FNPRM* Comments at 5.

<sup>21</sup> Cell Command *FNPRM* Comments at 2.

<sup>22</sup> See Inpixon *FNPRM* Comments at 5-8 (explaining that the contraband wireless devices issue extends well beyond CMRS frequencies and cell phones to [inter alia] Part 15 services and IoT devices).

### **C. Cell Command's Beacon Mandate is Anti-Competitive**

Basic tenets of economics, the FCC's specific institutional objectives, and broader regulatory principles also would advise against imposing a technology-specific government mandate. One of the FCC's fundamental goals as an agency is to promote competition amongst the services that fall within its jurisdiction.<sup>23</sup> While ensuring public safety is a co-equal goal with promoting competition for the Commission, in the context of combating the use of contraband wireless devices, these objectives are symbiotic rather than mutually exclusive. The Commission can best promote public safety by allowing correctional facilities to draw from a variety of CIS, MAS, and other solutions rather than mandating the use of a particular technology. According to Chairman Pai's regulatory philosophy as stated on his FCC bio, "regulators should be skeptical of pleas to regulate rivals, dispense favors, or otherwise afford special treatment."<sup>24</sup>

Cell Command's proposed beacon mandate runs contrary to widely accepted principles of competition policy. The record in this proceeding demonstrates that numerous solutions are available to correctional facilities, each with their own uses and limitations. As Global Tel\*Link noted, "a correctional facility should not be restricted from using the technical solution that best meets its specific and unique needs."<sup>25</sup> Accordingly, they acknowledge that "mandating a one-size-fits-all technical solution is not workable."<sup>26</sup> Beacons, CIS, MAS, and other solutions should not be treated as though they were mutually exclusive. These solutions can, and often do, work in tandem. As Prelude Communications observes, "it is important to

---

<sup>23</sup> FCC, *Strategic Plan of the FCC*, <https://www.fcc.gov/general/strategic-plan-fcc> (last visited July 9, 2017).

<sup>24</sup> FCC, *Ajit Pai Bio*, <https://www.fcc.gov/about/leadership/ajit-pai> (last visited July 9, 2017).

<sup>25</sup> GTL FNPRM Comments at 2.

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

have various technologies available to the correctional agencies to provide a layered security solution.”<sup>27</sup> However, rather than collaborative coexistence with other solutions in the marketplace, Cell Command seeks a government mandate for its offering.

Cell Command’s own recent demonstration before the Commission should give the agency pause before mandating an exclusive interdiction technology.<sup>28</sup> While Cell Command apparently demonstrated its ability to disable communications of various cell phones that were operating in airplane mode utilizing Wi-Fi, the demonstration did not address the threat of communications via Bluetooth (which Inpixon IPA detects, locates, and reports to appropriate authorities). However, even if Cell Command had addressed a broader range of communicative devices and frequencies in their demonstrations, it is important to recognize that device disabling – whether via beacon technology, carrier termination of service, or other means, is but one tool that should be available to correctional facilities. As Inpixon acknowledged in its initial comments, designated correctional facilities officers (“DCFOs”) may also want to draw on technologies such as Inpixon IPA’s data analytics platform in order to monitor and investigate patterns of illicit communications in their facilities rather than immediately disabling the contraband devices. This is all the more reason the Commission should not pigeonhole correctional facilities by locking them in with a single solution.

As Commissioner O’Rielly noted in his statement on the *FNPRM*, “the possibility that the Commission would mandate beacon technologies... is not a technology neutral approach.”<sup>29</sup> Rather than allowing correctional facilities discretion and choice, the Commission would effectively limit competition by mandating the use of a particular technology. As T-

---

<sup>27</sup> Prelude Communications *FNPRM* Comments at 2.

<sup>28</sup> See Ex Parte of Cell Command, GN Docket No. 13-111, at 2 (filed June 30, 2017) (“Cell Command Ex Parte”).

<sup>29</sup> *FNPRM*, Commissioner O’Rielly Statement at p. 100.

Mobile observed, “[Cell Command’s approach] would be inconsistent with the Commission’s policy against choosing technological winners and losers.”<sup>30</sup>

While Cell Command claims it only wants the FCC to create a voluntary process for industry adoption of its software, the company’s initial comments on the *FNPRM* belie such claims and lay bare their pursuit of a federal mandate. Part II of their comments claims that all other technological solutions for combating contraband wireless devices are fatally flawed.<sup>31</sup> Part III of said comments argues that their beacon solution is the only comprehensive solution in existence.<sup>32</sup> Finally, in Part IV, Cell Command provides several legal theories they claim would empower the Commission to mandate the use of its beacon technology.<sup>33</sup> Amongst its requests, Cell Command asserts that the Commission should issue a policy statement finding that its beacons are the “only effective solution.”<sup>34</sup> Inpixon is not opposed to the Commission convening equipment manufacturers, carriers, and other pertinent stakeholders in an effort to get industry to voluntarily adopt beacon software, but does not believe the Commission should single out beacons or any other technology as the “only effective solution.” Rather, the Commission should stay true to the Chairman’s regulatory philosophy by maintaining its longstanding policy of technological neutrality.

#### **IV. CONCLUSION**

Inpixon applauds the Commission for its continued efforts to fight back against the unauthorized use of wireless devices in prisons. Passive detection systems are the first line of defense and an indispensable source of intelligence in the fight against illicit communications.

---

<sup>30</sup> T-Mobile *FNPRM* Comments at 15.

<sup>31</sup> Prelude Communications *FNPRM* Comments at 7-16.

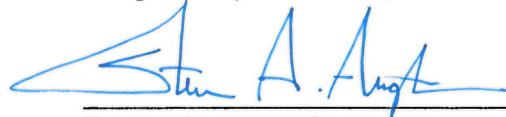
<sup>32</sup> *Id.*, at 16-19.

<sup>33</sup> *Id.*, at 19-26.

<sup>34</sup> Prelude Communications *FNPRM* Comments at 25-26.

Accordingly, their contributions should be recognized as falling within the scope of eligibility for Contraband Interdiction Systems. Furthermore, the Commission is already well versed in the drawbacks of picking winners and losers. As the communications technology landscape continues to evolve, so will the needs of correctional facilities in the struggle to combat unauthorized communications. For that reason, the Commission should refrain from locking in a single technology and allow correctional facilities to choose interdiction services for themselves.

Respectfully submitted,



---

Steven A. Augustino  
Ross G. Slutsky  
Kelley Drye & Warren LLP  
3050 K Street, NW  
Suite 400  
Washington, D.C. 20007-5108  
(202) 342-8612

*Counsel to Inpixon USA*

Dated: July 17, 2017