

**Before the  
Federal Communications Commission  
Washington, DC 20554**

In the Matter of	)	
	)	
Petition of American Hotel & Lodging	)	RM No. 11737
Association, Marriott International, Inc.	)	
and Ryman Hospitality Properties for a	)	
Declaratory Ruling to Interpret 47 U.S.C.	)	
§ 333, or, in the Alternative, for Rulemaking	)	

**OPPOSITION OF  
THE WIRELESS INTERNET SERVICE PROVIDERS ASSOCIATION  
TO PETITION FOR DECLARATORY RULING OR, IN THE  
ALTERNATIVE, FOR RULEMAKING**

Chuck Hogg, President  
Alex Phillips, FCC Committee Chair  
Jack Unger, Technical Consultant

Stephen E. Coran  
David S. Keir  
Lerman Senter, PLLC  
2000 K Street, NW, Suite 600  
Washington, D.C. 20006  
(202) 416-6744  
*Counsel to the Wireless Internet Service Providers Association*

December 19, 2014

**TABLE OF CONTENTS**

Summary ..... ii

Background and Statement of Interest ..... 2

Discussion ..... 3

I. THE COMMISSION SHOULD DISMISS THE PETITION AS BOTH ILL-FOUNDED AND UNNECESSARY, AFFIRMING BY SUCH ACTION THAT IT IS ILLEGAL TO BLOCK OR IMPAIR SERVICE TO AUTHORIZED WIRELESS DEVICES. .... 3

II. THERE IS NO NEED FOR A COMMISSION RULEMAKING RESPONDING TO PETITIONERS’ ALTERNATIVE REQUEST FOR RELIEF, AS PETITIONERS CAN ADDRESS LEGITIMATE THREATS TO THEIR NETWORKS WITHOUT CHANGES TO THE COMMISSION’S RULES..... 12

Conclusion ..... 15

## Summary

The Wireless Internet Service Providers Association (“WISPA”) hereby opposes the “Petition for Declaratory Ruling or, in the Alternative, for Rulemaking” (“Petition”) filed jointly by the American Hotel & Lodging Association, Marriott International, Inc. (“Marriott”) and Ryman Hospitality Properties (“collectively, “Petitioners”). The Commission should dismiss the Petition as a transparent attempt to permit commercial establishments to interfere intentionally with lawful devices operating *on other networks*. No amount of misdirection can save Petitioners from the indisputable fact that Section 333 of the Communications Act of 1934, as amended (the “Act”) expressly forbids the willful and malicious interference that Petitioners seek to legitimize under the guise of network management. Nor should the Commission grant Petitioners’ alternative request for a rulemaking proceeding. Rather, the Commission should reiterate that the law prohibits blocking, jamming or other intentional acts designed to disrupt lawful Part 15 communications devices.

As the trade association representing the interests of wireless Internet service providers (“WISPs”) that rely on unlicensed spectrum to deliver fixed broadband services to homes, businesses and first responders, WISPA has a strong interest in this proceeding. It is concerned that approving Petitioners’ request would not only violate the law, but would lead to massive disruption of wireless devices that people rely on every day for emergency and other communications.

Petitioners wrongly assert that Section 333 has not been interpreted to prohibit interference to Part 15 devices. To the contrary, the Commission has consistently stated that Section 333 prohibits “devices that intentionally block, jam or interfere with authorized radio

communications” (see page 4, *infra*, & n.8) and has sanctioned multiple companies – including Marriott – for actions contrary to Section 333.

Despite their admission on the Petition’s first page that the actions for which they seek approval “may result in ‘interference with or cause interference’ to a Part 15 device being used by a guest on the operator’s property,” Petitioners nevertheless attempt to distinguish the operation of “Wi-Fi monitoring equipment” from the use of devices that are intended solely to interfere with communications signals. Wi-Fi monitoring equipment serves a legitimate and legal purpose when used to manage the internal traffic demands of a wireless network, but does not make its use *to interfere with other networks or devices* permissible or “FCC-approved.”

Likewise, Petitioners’ selective reliance on Section 333’s legislative history is contravened by the broad statutory language. This language identifies protected uses subject to license or directly “authorized by the Act” as well as those authorized “under” the Act, which clearly includes Part 15 devices that have been authorized since 1938, long before the adoption of Section 333. Had Congress intended to limit the prohibition on willful or malicious interference, it would not have used the broad, inclusive language of Section 333.

Petitioners also attempt to equate *incidental* interference, which may occur even when all parties are lawfully operating, with *intentional* interference, which is the conduct prohibited under Section 333. This misinterpretation flies in the face of the plain meaning of Section 333 and the Commission’s consistent application of that language in prohibiting intentional interference to Part 15 devices.

At the same time, Petitioners ignore the practical realities that would result from allowing hotels and other commercial establishments to intentionally disrupt operations on other wireless networks. Emergency calls would be blocked, GPS location services could be inoperable and

normal voice services would be disrupted, all at the discretion of a business acting in its own self-interest.

Wi-Fi access operators should be able to manage their own network capacity and prevent connections to their network that impair others use of their service, but they should not be permitted to impair services operated by other parties under the guise of “management.” The Commission should reaffirm that a party using Wi-Fi monitoring equipment may do so only to manage its own network for reliability (*e.g.*, avoiding congestion) or to identify a legitimate security threat that poses a risk to users of its *own* network, and not to interfere intentionally with the operations of lawful devices on *other* networks.

**Before the  
Federal Communications Commission  
Washington, DC 20554**

In the Matter of	)	
	)	
Petition of American Hotel & Lodging Association, Marriott International, Inc. and Ryman Hospitality Properties for a Declaratory Ruling to Interpret 47 U.S.C. § 333, or, in the Alternative, for Rulemaking	)	RM No. 11737

**OPPOSITION OF  
THE WIRELESS INTERNET SERVICE PROVIDERS ASSOCIATION  
TO PETITION FOR DECLARATORY RULING OR, IN THE  
ALTERNATIVE, FOR RULEMAKING**

The Wireless Internet Service Providers Association (“WISPA”), pursuant to Section 1.405(a) of the Commission’s Rules, hereby opposes and requests dismissal of the above-captioned “Petition for Declaratory Ruling or, in the Alternative, for Rulemaking” (“Petition”) filed jointly by the American Hotel & Lodging Association, Marriott International, Inc. (“Marriott”) and Ryman Hospitality Properties (“Ryman”) (collectively, “Petitioners”).<sup>1</sup> Despite their attempt to cast their request as a necessity for management of *their* networks, Petitioners seek, in effect, a broad right for commercial establishments to manage wireless networks that are *not* their own by intentionally interfering with and disabling lawful devices. For the reasons discussed below, the Commission should dismiss the Petition as both unnecessary and unfounded, reaffirming that any actions taken by anyone to jam, block or otherwise interfere with authorized wireless communications on other devices or networks violates Section 333 of the Communications Act of 1934, as amended (the “Act”). Given the lack of foundation for the

---

<sup>1</sup> See *Public Notice*, Report No. 3012 (rel. Nov. 19, 2014).

relief requested in the Petition, and the perfunctory and non-specific alternative request for rulemaking, the Commission also should decline to initiate a rulemaking proceeding in response to the Petition. The Petition raises no issues that require further Commission consideration.

### **Background and Statement of Interest**

WISPA is the trade association that represents the interests of wireless Internet service providers (“WISPs”) that provide fixed wireless broadband services to consumers, businesses and first responders across the country. WISPs rely principally on unlicensed spectrum in the 900 MHz, 2.4 GHz and 5 GHz bands, along with “lightly licensed” spectrum in the 3650-3700 MHz band, to deliver fixed broadband services. These bands are shared with other WISPs, industrial users such as smart grid companies, and consumer devices such as baby monitors, garage door openers, cordless telephones and home Wi-Fi networks. WISPs have demonstrated an ability to coordinate and share spectrum with other users through channel planning, antenna cross-polarization, sectorization and other interference mitigation and avoidance techniques.

WISPA is concerned that the relief requested in the Petition squarely contravenes the Act and, in particular, established Commission policies and enforcement actions implementing its clear authority under Section 333 of the Act.<sup>2</sup> Indeed, the Commission has already taken enforcement action against one of the Petitioners, Marriott, determining that it violated Section 333 when its employees blocked the signals of Wi-Fi devices in use at the Marriott-managed and Ryman-owned Gaylord Opryland Hotel and Convention Center in Nashville, Tennessee.<sup>3</sup> The Petitioners seek to vitiate the statutory protections provided by Section 333, a step that would be

---

<sup>2</sup> Section 333 provides in its entirety: “No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized under this chapter or operated by the United States Government.” 47 U.S.C. § 333.

<sup>3</sup> See *Marriott International, Inc., et al.*, 29 FCC Rcd 11760 (2014) (“*Marriott Order*”); *Marriott International, Inc., et al.*, 29 FCC Rcd 11762 (2014) (“*Marriott Consent Decree*”).

extremely disruptive to those using authorized wireless devices to receive reliable and secure communications. Indeed, under the carte blanche “right to interfere” that Petitioners seek, there would be no way to prevent *any* commercial establishment from blocking wireless communications, thereby depriving consumers of the benefits of the lawful wireless devices and networks they choose to use. The Commission therefore must continue to apply Section 333 of the Act as written to prohibit the unfair and destructive practices that Petitioners seek to legitimize.

### Discussion

#### **I. THE COMMISSION SHOULD DISMISS THE PETITION AS BOTH ILL-FOUNDED AND UNNECESSARY, AFFIRMING BY SUCH ACTION THAT IT IS ILLEGAL TO BLOCK OR IMPAIR SERVICE TO AUTHORIZED WIRELESS DEVICES.**

The Petition is filed with the Commission as a request for a declaratory ruling or order pursuant to both Section 554(e) of the Administrative Procedure Act and Section 1.2 of the Commission’s Rules.<sup>4</sup> These provisions make clear that the agency is empowered to “issue a declaratory order to terminate a controversy or remove uncertainty.”<sup>5</sup> Issuing such an order would be inappropriate in this instance because there is neither controversy nor uncertainty concerning the matter addressed by the Petition – the applicability of the Section 333 prohibition on intentional interference to devices authorized under Part 15 of the Commission’s Rules.

Specifically, the essential claim underpinning the Petition, repeated at several points, is that “the FCC has never interpreted Section 333 to prohibit interference to Part 15 devices or

---

<sup>4</sup> See 5 U.S.C. § 554(e); 47 C.F.R. § 1.2.

<sup>5</sup> 5 U.S.C. § 554(e). The Commission’s Rules include nearly identical language, but refer to a “declaratory ruling” instead of a “declaratory order.”

found a violation of Section 333 based upon such interference.”<sup>6</sup> In fact, this statement is patently untrue. The Commission’s appropriate application of its broad authority under Section 333 to Part 15 wireless networking equipment was not only clear before the Petition was filed, but has been reaffirmed in the interim in an Order involving two of the Petitioners, Marriott and Ryman.<sup>7</sup>

More than three years ago, for example, the Commission released a pair of Enforcement Advisory Public Notices identifying Wi-Fi networking gear as part of a list of communications equipment covered by Section 333’s prohibition against using “devices that intentionally block, jam, or interfere with authorized radio communications.”<sup>8</sup> Subsequent to these general notices, multiple companies have been cited or found liable for monetary forfeiture for marketing devices that are ineligible for Commission authorization or certification precisely because their use to interfere with radio communications would violate Section 333 of the Act. The uses targeted by

---

<sup>6</sup> Petition at 14; *see also* Petition at 20 (“the Commission has never previously interpreted Section 333 to prohibit interference to Part 15 devices”).

<sup>7</sup> *See Marriott Order* at 11760 1 (¶ 1); *Marriott Consent Decree* at 11763 (¶ 2) & 11764 (¶ 6).

<sup>8</sup> *FCC Enforcement Advisory*, “Cell Jammers, GPS Jammers, and Other Jamming Devices,” 26 FCC Rcd 1329, DA 11-250, Enforcement Advisory No. 2011-04 (released Feb. 9, 2011) (“We remind consumers that it is a violation of federal law to use devices that intentionally block, jam, or interfere with authorized radio communications such as cell phones, police radar, GPS, and Wi-Fi”) (emphasis in original); *FCC Enforcement Advisory*, “Cell Jammers, GPS Jammers, and Other Jamming Devices,” 26 FCC Rcd 1327, DA 11-249, Enforcement Advisory No. 2011-03 (released Feb. 9, 2011) (“This longstanding prohibition applies to any type of jamming equipment, including devices that interfere with cellular and Personal Communications Services (PCS), police radar, Global Positioning systems (GPS), and wireless networking services (Wi-Fi)”). Wi-Fi communications equipment is not licensed by the Commission, but is authorized on an unlicensed basis pursuant to Part 15 of the Commission’s Rules. *See* 47 C.F.R. §§ 15.1 *et seq.*

these unlawful jammers included several types of Part 15 devices, including Wi-Fi, Bluetooth and remote control equipment.<sup>9</sup>

In addition, as noted above, a few months after filing the Petition, Marriott itself entered into a Consent Decree with the FCC's Enforcement Bureau settling the Bureau's investigation concerning interference with Wi-Fi networks in violation of Section 333.<sup>10</sup> While Marriott does not admit therein that its actions – deactivating Wi-Fi Internet access points that were not part of its system at the Gaylord Opryland Hotel – were a violation of Section 333, the Consent Decree makes plain the Bureau's view, consistent with precedent, that Marriott's actions violated the law.<sup>11</sup>

Petitioners miss the point in attempting to distinguish conduct in the operation of “Wi-Fi monitoring equipment” from the use of devices that are intended solely to jam communications signals.<sup>12</sup> Though Wi-Fi monitoring equipment serves a legitimate and legal purpose when used to manage the internal traffic demands of a wireless network, that does not make its use *to interfere with other networks or devices* permissible or “FCC-approved.” Any equipment, whether or not it is approved by the Commission, used willfully or maliciously to cause

---

<sup>9</sup> See *C.T.S. Technology Co., Limited*, 29 FCC Rcd 8107, 8111 (¶ 12) (2014) (citing Section 333 in imposing a large forfeiture against a company that marketed multiple jamming devices, including those designed to interfere with Wi-Fi equipment); *Illegal Marketing of Signal Jamming Devices*, Omnibus Citation and Order, 26 FCC Rcd 13565, 13566-67 (¶¶ 5&6) (EB 2011) (citing twenty different online vendors for marketing of jamming equipment in violation of Section 333, including citations for more than three dozen products that blocked Wi-Fi signals, at least a half-dozen of which jammed Wi-Fi and/or Bluetooth frequencies exclusively; in addition, two of the cited jamming devices were intended to interfere solely with unlicensed remote controls operating in the 315 MHz and 433 MHz bands).

<sup>10</sup> See *Marriott Consent Decree* at 11769 (¶ 24); *Marriott Order* at 11760 (¶ 1).

<sup>11</sup> *Id.* at 3 (¶ 6). See also *FCC Public Notice*, “Marriott to Pay \$600,000 to Resolve Wi-Fi-Blocking Investigation,” released October 3, 2014 (“It is unacceptable for any hotel to intentionally disable personal hotspots ... Marriott must cease the unlawful use of Wi-Fi blocking technology”).

<sup>12</sup> See *Petition* at 3-4 & 18 n.37.

interference to radio communications violates the law.<sup>13</sup> Petitioners admit at the outset of the Petition that the actions for which they seek approval “may result in ‘interference with or cause interference’ to a Part 15 device being used by a guest on the operator’s property.”<sup>14</sup>

Although the applicable precedents by themselves are sufficient to undermine the central premise of the Petition, allowing the Commission to dismiss it with prejudice, it bears emphasis that none of Petitioners’ ancillary arguments survives scrutiny. Petitioners resort to a contorted and selective review of Section 333’s legislative history and a misinterpretation of the Commission’s own Part 15 regulations in an effort to buttress their misdirected request for relief.<sup>15</sup> Specifically, the Petition advances theories that: (1) the Act itself did not specifically mention unlicensed devices in 1990, when Section 333 was adopted, so these devices could not reasonably be included within its protections;<sup>16</sup> (2) the House and Senate Reports discussing Section 333’s adoption express “concern about interference to certain types of radio communications services,” and only these services are intended to be protected;<sup>17</sup> and (3) Part 15 devices must accept interference from other lawfully operating communications equipment, both

---

<sup>13</sup> Willful and malicious interference is not limited to jamming, as the legislative history of the provision makes clear. The House Committee report states that the statutory language prohibits “intentional jamming, deliberate transmission on top of the transmissions of authorized users already using specific frequencies in order to obstruct their communications, repeated interruptions, and the use and transmission of whistles, tapes, records, or other types of noisemaking devices to interfere with the communications or radio signals of other stations.” H.R. Rep. No. 101-316 at 9 (1990).

<sup>14</sup> See Petition at 1.

<sup>15</sup> If Petitioners disagree with the scope of the statutory protections, their remedy would be to change the law by seeking Congressional action.

<sup>16</sup> See Petition at 4-5 & 14-15.

<sup>17</sup> See *id.* at 5 & 15-16.

licensed and unlicensed, precludes protection against intentional interference.<sup>18</sup> All of these arguments lack merit.

First, it is immaterial whether the Act itself specifically referenced unlicensed devices in 1990. The statutory language refers not only to uses subject to license or directly “authorized by the Act,” but those authorized “under” the Act as well.<sup>19</sup> There is no question that Part 15 devices are authorized by the Commission pursuant to its authority under the Act, and that their regulatory authorization and use long predates the 1990 adoption of Section 333.<sup>20</sup> Indeed, the Petitioners themselves note that “the FCC’s Part 15 rules had been in place for more than 50 years when Section 333 was enacted in 1990.”<sup>21</sup> Both before and after the adoption of Section 333, Congress has acknowledged the legal basis for operation of the many significant consumer products that are authorized under Part 15.<sup>22</sup> Moreover, as noted above, the Commission has explicitly referenced the applicability of Section 333 with respect to the jamming of unlicensed

---

<sup>18</sup> *See id.* at 5 & 16-17.

<sup>19</sup> 47 U.S.C. § 333.

<sup>20</sup> *See, e.g., Revision of Part 15 of the Commission’s Rules Regarding Ultra-Wideband Systems*, 19 FCC Rcd 24558, 24590 (¶ 69) (2004) (“The Commission first adopted rules for unlicensed operation of low power radio devices in 1938, and the basic construct of this regulatory regime continues to apply today”). *See also* 47 U.S.C. § 303(r) (Commission empowered to “[m]ake such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this chapter”).

<sup>21</sup> *See* Petition at 16.

<sup>22</sup> For example, in its adoption of the Electronic Communications Privacy Act of 1986, Congress noted in the legislative record that cordless telephones “are regulated under Part 15, Subpart E of the rules of the Federal Communications Commission (FCC), and are not licensed.” P.L. 99-508, H. Rep. 99-647, 99<sup>th</sup> Cong., 2d Sess., at 33 (June 19, 1986). *See also* *Hernstadt v. FCC*, 677 F.2d 893, 902 n.22 (D.C. Cir. 1980) (Congress is presumed to be cognizant of, and legislate against background of, existing agency interpretation of law).

Wi-Fi radio communications, both in enforcement advisory public notices<sup>23</sup> and in adjudicative orders.

Second, Petitioners are wide of the mark in attempting to argue that the reference in the House Committee Report of specific services that were experiencing willful interference as of 1990 evidenced an intent by Congress to limit the scope of Section 333. Certainly, had Congress intended to apply the prohibition on willful or malicious interference only to specific services, it would have clearly enumerated these services in the new provision.<sup>24</sup> Section 333 does not include such limiting language. Indeed, both the broad language of Section 333 and the provision's legislative history make clear that the scope of this prohibition was intended to be expansive.

It is a foundational requirement of statutory interpretation that effect be given to the plain language of the statute.<sup>25</sup> The statute plainly states, without exception, that “No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States

---

<sup>23</sup> See also *FCC Enforcement Advisory*, “WARNING: Jammer Use is Prohibited,” DA 14-1785, Enforcement Advisory No. 2014-05 (released Dec. 8, 2014) (“2014 Advisory”) (“For example, jammers can ... prevent your Wi-Fi enabled device from connecting to the Internet”).

<sup>24</sup> See, e.g., *Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 373 (1986) (Congress' choice of broad statutory language demonstrates a statute's intended breadth of application); *Consumer Electronics Ass'n v. FCC*, 347 F.3d 291, 298 (D.C. Cir. 2003) (“statutes written in broad, sweeping language should be given broad, sweeping application”). Cf. *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984) (“considerable weight should be accorded to an executive department's construction of a statutory scheme it is entrusted to administer”) (“*Chevron*”).

<sup>25</sup> See, e.g., *Ratzlaf v. U.S.*, 510 U.S. 135, 147-48 (1994) (“we do not resort to legislative history to cloud a statutory text that is clear”); *Chevron*, 467 U.S. at 842-43 (where Congress “has directly spoken to the precise question at issue,” effect must be given to its “unambiguously expressed intent”).

Government.”<sup>26</sup> Almost every element of the text is intended to broaden the scope of protection, with the only words of limitation being the restriction of the proscription to intentional interference – *i.e.*, interference that is “willfully or maliciously undertaken.”<sup>27</sup> “No person” may engage in such conduct, and the protection applies to “any radio communications” of “any station” whether such station is “licensed” or “authorized” “by or under” the Act or by the Federal government.<sup>28</sup> This plain meaning is buttressed by the Committee Report issued by the House Energy and Commerce Committee in connection with the House bill, H.R. 3265, which unambiguously states the Committee’s finding that “placement of the proposed *general prohibition against interference* in the Act, in addition to elevating the gravity of such violations, will increase public awareness of the prohibition against this particularly disruptive type of violation.”<sup>29</sup> Section 333 thus is unmistakably intended to be a general prohibition against intentional interference with any FCC-authorized communication.

Third, Petitioners offer various assertions to suggest that services offered using Part 15 devices cannot be protected from willful or malicious interference. They argue that the rules expressly state that “harmful interference” requires the interruption of a “radiocommunications service.”<sup>30</sup> In addition, Petitioners contend that a Part 15 device must itself “accept whatever interference is received.”<sup>31</sup> These arguments are fundamentally misplaced as they confuse *incidental* interference, including harmful interference, which may occur even when all parties

---

<sup>26</sup> 47 U.S.C. § 333.

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

<sup>28</sup> *Id.* The term “station,” in turn, is defined broadly to encompass any “equipped to engage in radio communication or radio transmission of energy.” 47 U.S.C. § 153(42).

<sup>29</sup> H.R. Rep. No. 101-316 at 9 (1990).

<sup>30</sup> *See* Petition at 16.

<sup>31</sup> *See id.*

are operating in a manner fully consistent with FCC rules, with *intentional* interference, which is the conduct prohibited under Section 333. Part 15 devices are required to operate in whatever interference environment they are placed and may not cause harmful interference to licensed spectrum users, but the law does not place the users of these devices at the mercy of any person who seeks to intentionally disrupt their use. Petitioners therefore cannot use the potential for unintentional harmful interference as a pretext for deliberate and disruptive interference of service to other Part 15 devices.<sup>32</sup>

Petitioners also distort reality by asserting that Section 333 would make violators out of any person who uses a Part 15 device that inadvertently interferes with another such device.<sup>33</sup> In making a call with a cordless telephone, for example, the user's intent is only to complete the call, not to interfere with the use of another nearby device. By contrast, any party that uses Wi-Fi monitoring equipment to "cleanse" the premises of other legally operating Wi-Fi devices not connected to its network is engaged in an act of premeditated and purposeful interference.

With respect to this final point, Petitioners' arguments invoking the Commission's rules concerning Over-the-Air Reception Devices ("OTARD") are also misplaced. Petitioners appear to argue that affording individuals, such as hotel guests, a right to be free from interference when using their personal communications devices on another's property, in this case a hotel, would somehow give them "superior rights as compared to owners or lessors."<sup>34</sup> This argument is mistakenly premised on the fact that the invocation of substantively different rights under OTARD requires one to have an ownership or leasehold interest in the premises. This is an

---

<sup>32</sup> See, e.g., *Continental Airlines*, 21 FCC Rcd 13201, 13214 (¶ 30) (2006) (finding that the operator of a Wi-Fi backbone composed of Part 15 devices (Massport) has no "right" to operate it free from interference from other Part 15 devices (deployed by Continental Airlines)).

<sup>33</sup> See Petition at 17.

<sup>34</sup> See Petition at 5-6 & 19.

apples-to-oranges comparison, as OTARD has nothing to do with the transient presence of a device that may function as an access point, or the use by an individual of his or her own mobile phone, tablet or laptop to access wireless services that may be available at a given location. Section 333 affords protection from intentional interference to the providers of services that such transient users may access, as well as the device users themselves, but it does not afford any of them the right to install or maintain permanent facilities on someone else's property. The OTARD rules, on the other hand, protect the specific rights of property owners or leaseholders physically to install communications equipment in the face of arbitrary restrictions, such as zoning laws and homeowners' association covenants restricting use based solely on aesthetic considerations.<sup>35</sup>

Allowing commercial Wi-Fi network operators to interfere willfully with the lawful operation of communications equipment would potentially wreak havoc upon neighboring businesses and legitimate consumer expectations. While Petitioners maintain that they do not seek "to mitigate operations occurring outside the premises of a Wi-Fi network operator,"<sup>36</sup> they fail to explain how disabling devices that are not connected to their own network would not adversely impact both nearby users and other nearby service providers making lawful use of Wi-Fi networks and devices. Moreover, they do not articulate with any specificity how disruption to off-site devices would be avoided under these circumstances. Accordingly, to the extent that Petitioners seek a declaratory ruling that intentional interference with Wi-Fi devices on their property is consistent with Section 333 of the Act, their request must be roundly rejected as both unfounded and contrary to the Act and Commission precedent.

---

<sup>35</sup> See 47 C.F.R. § 1.4000.

<sup>36</sup> Petition at 9 n. 11.

Aside from the legal infirmities inherent in the Petition, there are significant policy reasons why the Commission should not approve actions taken by a hotel, or any commercial establishment, that would sanction intentional interference to the operation of authorized devices. Consumers use their devices to communicate important information in a reliable way, and such devices are critical for public safety. As the Commission stated in the *2014 Advisory*:

Jammers can prevent 9-1-1 and other emergency phone calls made by the public from getting through to first responders or interfere with police and other law enforcement communications that are critical to the carrying out of law enforcement missions. Jammers also prevent the public, including individuals and businesses, from engaging in any of the myriad lawful forms of communications that occur constantly in all corners of the country – simple one-on-one phone conversations, communication among persons in large groups (such as during lawful rallies and protests), use of GPS-based map applications, social media use, etc.<sup>37</sup>

Moreover, granting the Petitioners the broad relief they seek would be an open invitation to *any* business to intentionally interfere with the devices of their customers, guests and others, for any reason they deem fit. The ramifications of this proceeding extend far beyond a hotel or a convention center, and the Commission should not begin sliding down the slippery slope to endorse outcomes even more absurd than the one sought here.

**II. THERE IS NO NEED FOR A COMMISSION RULEMAKING RESPONDING TO PETITIONERS' ALTERNATIVE REQUEST FOR RELIEF, AS PETITIONERS CAN ADDRESS LEGITIMATE THREATS TO THEIR NETWORKS WITHOUT CHANGES TO THE COMMISSION'S RULES.**

With Petitioners' faulty premises and flimsy arguments exposed, there is no uncertainty that requires any Commission action apart from dismissing the Petition. Petitioners may not interfere with the operation of Wi-Fi devices that are not part of their own networks. Any business practices that the Petitioners may wish to undertake must be related only to the internal

---

<sup>37</sup> *2014 Advisory* at 1.

integrity of their *own* communications networks, and the Commission should so state in its Order dismissing the Petition.

Although Petitioners ask, in the alternative, for the Commission to institute a rulemaking to clarify what they are permitted to do in order to manage their own Wi-Fi services,<sup>38</sup> the scope of permitted conduct is unambiguous and does not require validation through any Commission action. The questions that the Petition poses in this regard are susceptible to practical answers, are beyond the scope of the Petitioners' reasonable concern, or would cause the Commission to engage in speculation about future cases that cannot be foreseen. The Petition, for example, poses the question whether it is "appropriate for a university to limit a student's ability to use a Wi-Fi network for bandwidth intensive services and applications."<sup>39</sup> It also raises the question of how a property owner can prevent an unauthorized access point from "spoofing," or passing itself off as an official access point, for the purpose of gathering users' confidential information.<sup>40</sup> In addition, it asks whether it is permissible for a hotel to take action against an unauthorized access point plugged into the hotel's wired network that poses a security threat.<sup>41</sup>

It should be self-evident that an effective response to each of the concerns raised does not require a Wi-Fi network operator to cause intentional interference that could disrupt not only the intended target, but nearby lawful Wi-Fi networks and devices as well. Excessive bandwidth use can be legally managed by the network operator consistent with terms of service that allow system administration to assure an acceptable level of service for all users. Any access point that

---

<sup>38</sup> See Petition at 6 & 19-21.

<sup>39</sup> See Petition at 21. The Petition does not explain why a lodging trade association, a hotel operator, and a property owner seek guidance on how a university may operate its Wi-Fi networks.

<sup>40</sup> See Petition at 21.

<sup>41</sup> *Id.*

engages in fraud by attempting to “spoof” a hotel or other commercial Wi-Fi network for the purpose of gathering users’ personal data can be identified and shut down with the assistance of law enforcement. A wireless device that is *connected* to a wired network in a way that compromises security can be identified and de-authenticated individually, in the event that it poses a security risk, without interfering with other devices.

In short, those operating Wi-Fi access networks should be able to manage their own network capacity and prevent connections to their network that impair others use of the service,<sup>42</sup> but they should not be permitted to “manage” or otherwise impair services operated by other parties in an effort to mitigate incidental interference.<sup>43</sup> The Commission should reaffirm that a party using Wi-Fi monitoring equipment may do so only to manage its own network for reliability (*e.g.*, avoiding congestion) or to identify a legitimate security threat that poses a risk to users of its *own* network.

---

<sup>42</sup> Indeed, the Petitioners specifically reference such types of functionality in describing the utility of Wi-Fi monitoring equipment. *See* Petition at 9 (referencing its ability “to identify what types of devices are on its network, where the devices are accessing the network, and the bandwidth they consume”).

<sup>43</sup> *See Continental Airlines*, 21 FCC Rcd at 13214 (¶ 30) and note 33, *supra*.

## **Conclusion**

For all of the foregoing reasons, WISPA urges the Commission to dismiss the Petition for Declaratory Ruling and to terminate this proceeding, reaffirming in the process that the statutory prohibition on willful or malicious interference applies to all radio communication equipment authorized under the Commission's Rules.

Respectfully submitted,

### **WIRELESS INTERNET SERVICE PROVIDERS ASSOCIATION**

December 19, 2014

By: */s/ Chuck Hogg, President*  
*/s/ Alex Phillips, FCC Committee Chair*  
*/s/ Jack Unger, Technical Consultant*

Stephen E. Coran  
David S. Keir  
Lerman Senter, PLLC  
2000 K Street, NW, Suite 600  
Washington, D.C. 20006  
(202) 416-6744  
*Counsel to the Wireless Internet Service Providers Association*

**CERTIFICATE OF SERVICE**

I, Sharon Krantzman, hereby certify that on this 19<sup>th</sup> day of December 2014, a copy of the foregoing document was sent by first-class, postage prepaid mail to the following:

Banks Brown, Esquire  
McDermott Will & Emery LLP  
340 Madison Avenue  
New York, NY 10173  
*Counsel for the American Hotel and Lodging Association*

Bennett L. Ross, Esquire  
Wiley Rein LLP  
1776 K Street, NW  
Washington, DC 20006  
*Counsel for Marriott International, Inc. and Ryman Hospitality Properties*

/s/ Sharon Krantzman  
Sharon Krantzman