Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Petition of American Hotel & Lodging	)	
Association, Marriott International, Inc., and	)	RM-11737
Ryman Hospitality Properties for a Declaratory	)	
Ruling to Interpret 47 U.S.C. 333, or, in the	)	
Alternative, for Rulemaking	)	

COMMENTS OF CTIA–THE WIRELESS ASSOCIATION®

Michael F. Altschul
Senior Vice President & General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Brian M. Josef
Assistant Vice President, Regulatory Affairs

CTIA – The Wireless Association®
1400 16th Street, N.W., Suite 600
Washington, D.C. 20036
(202) 785-0081

December 19, 2014

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Petition of American Hotel & Lodging	)	
Association, Marriott International, Inc., and	)	RM-11737
Ryman Hospitality Properties for a Declaratory	)	
Ruling to Interpret 47 U.S.C. 333, or, in the	)	
Alternative, for Rulemaking	)	

COMMENTS OF CTIA–THE WIRELESS ASSOCIATION®

CTIA–The Wireless Association® ("CTIA"), pursuant to the November 19, 2014, Public Notice issued by the Consumer and Governmental Affairs Bureau,[1] hereby submits its comments on the above-referenced Petition filed by the American Hospitality & Lodging Association; Marriott International, Inc.; and Ryman Hospitality Properties (collectively, the "Petitioners").[2] CTIA recognizes and appreciates that Wi-Fi operators have legitimate needs to manage their networks to protect them from malicious interference. However, as described below, the Commission should deny Petitioners' request to give network operators blanket authority to shut down any and all Part 15 devices, including those that are being lawfully operated under the FCC's rules, which would violate Section 333 of the Communications Act of 1934 (the "Act") and the FCC's rules.

1/ *See Consumer & Governmental Affairs Bureau Reference Information Center Petition for Rulemaking Filed*, Public Notice, RM-11737, Report No. 3012 (rel. Nov. 19, 2014).

2/ *See* 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, *attached to* Letter from Bennett L. Ross, Wiley Rein LLP, Counsel to American Hotel & Lodging Association, *et al.*, to Ms. Marlene H. Dortch, Secretary, FCC, RM-11731 (filed Aug. 25, 2014) ("Petition").

I. INTRODUCTION AND SUMMARY

The wireless industry has long relied on unlicensed spectrum to support carrier operations and improve the customer experience. As CTIA has previously explained, the U.S. wireless industry employs a range of sophisticated techniques to maximize the efficiency and performance of its networks, including Wi-Fi offload to improve network coverage and increase capacity for voice and data traffic.[3] Wireless service providers not only have deployed thousands of Wi-Fi hotspots across the Nation to boost network capacity, but some now also offer consumer Wi-Fi calling options.[4] In fact, many mobile phone offerings provide voice communications primarily, and in some cases nearly exclusively, over Wi-Fi spectrum.[5] CTIA therefore has a strong interest in ensuring that unlicensed spectrum remains available to carriers unfettered by intentional interference.

CTIA understands Wi-Fi operators' interest in maintaining the security of their networks and address malicious attacks.[6] However, Wi-Fi operators may not "deputize" themselves to

---

3/ *See, e.g.*, Rysavy Research, *Efficient Use of Spectrum*, at 5 (May 4, 2011), *attached* to Letter from Christopher Guttman-McCabe, Vice President, Regulatory Affairs, CTIA, to Hon. Julius Genachowski *et al*., FCC, GN Docket No. 09-51, ET Docket Nos. 10-235, 10-237, at 1-2 (filed May 5, 2011) ("CTIA Rysavy Letter"); Comments of CTIA–The Wireless Association®, GN Docket No. 12-268, at 9 (filed Jan. 25, 2013) ("CTIA Incentive Auction Comments"); *see also* CTIA–The Wireless Association® Response to House White Paper on Modernizing U.S. Spectrum Policy, at 15 (filed Apr. 25, 2014) ("CTIA Spectrum White Paper Comments"), *available at* http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/analysis/CommActUpdate/WP2_Responses_14-25.pdf ("Unlicensed spectrum also has an important role to play in the wireless ecosystem. Wireless carriers often use unlicensed spectrum for, among other purposes, offloading traffic from their networks.").

4/ *See* Paul Barbagallo and Tim McElgunn, *Wi-Fi, Once a Lifeline for Mobile Carriers, Is Now a Threat*, Bloomberg BNA (May 28, 2014), *available at* http://www.bna.com/wifi-once-lifeline-n17179890780/; *see also, e.g.*, T-Mobile Release, *T-Mobile Launches Un-carrier 7.0 Un-leashes Wi-Fi Worldwide*, T-Mobile (Sept. 10, 2014), *available at* http://newsroom.t-mobile.com/news/t-mobile-launches-un-carrier-7.htm.

5 *See, e.g.*, Republic Wireless, FAQs, https://republicwireless.com/faqs (last visited Dec. 14, 2014).

6 The Petition was filed in the wake of a 2013 investigation initiated by the FCC's Enforcement Bureau ("Bureau") to determine whether use of a "network management system" with a de-authentication function, described more fully below, by one of the Petitioners – Marriott International, Inc. ("Marriott")

police the Part 15 radiofrequency environment. Section 333 of the Act prohibits intentional, targeted interference to transmissions, regardless of whether they are licensed or unlicensed under the Commission's rules. In addition, all Part 15 devices, including mobile devices that incorporate Part 15 capabilities, have equal rights to use unlicensed spectrum; no single entity may intentionally prevent others from using that spectrum. The Commission should therefore declare that the type of blanket de-authentication contemplated by the Petition violates the Act and the FCC's rules. The public interest also supports such an interpretation of Section 333 and the rules. To the extent Wi-Fi operators have a legitimate need to protect their networks, they have a variety of other tools available to them that do not involve unlawfully disabling third-party access points.

II. THE TYPE OF BLANKET DE-AUTHENTICATION PROPOSED IS PROHIBITED BY STATUTE AND RULE

The Petitioners state that because Wi-Fi networks are susceptible to a variety of attacks, any of which can be accomplished by an individual utilizing a Wi-Fi hotspot, many hotels utilize "network management systems" in order to ensure that guests and conference attendees have secure and reliable access to the Wi-Fi services they provide.[7] These network management systems typically allow hotels to monitor their systems by identifying the types of devices that are on the network, where the devices access the network, and the bandwidth that they consume.[8] However, some of these systems also include a function that allows the hotel to contain

---

– violated Section 333 of the Act. *See Marriott International, Inc. and Marriott Hotel Services, Inc.*, Order, 29 FCC Rcd. 11760 (2014) ("*Marriott Order*"). During the course of its investigation, the Bureau discovered that one or more Marriott employees used the de-authentication function in violation of Section 333 to prevent users from connecting to the Internet via their own personal Wi-Fi hotspots, even when they did not pose a security threat to the hotel's network. The Bureau and Marriott entered into a Consent Decree after the submission of the Petition. *See Marriott International, Inc. and Marriott Hotel Services, Inc.*, Consent Decree, 29 FCC Rcd. 11762 (2014) ("*Marriott Consent Decree*").

7/ *See* Petition at 2, 6-7.

8/ *See* Petition at 8-9.

unauthorized access points and send de-authentication packets that will prevent Part 15 devices from connecting to the unauthorized access points.[9] Use of that de-authentication feature is prohibited by statute and rule.

A. Blanket De-Authentication is Contrary to Section 333 of the Act

Section 333 provides that "[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government."[10] The Commission should declare that the type of de-authentication described by the Petition is prohibited by Section 333 of the Act. That interpretation is consistent with the legislative history of Section 333, which makes clear that *intentional disruptions* of a target's operations are prohibited, and the Commission's prior actions under Section 333.[11] As described, a de-authentication function does exactly what Congress sought to prohibit – intentional disruptions.

The Petitioners argue that Section 333 was not intended to prohibit interference to a Wi-Fi access point or any Part 15 device.[12] They assert that, by the statute's terms, Section 333 only safeguards stations "licensed or authorized by or under this chapter," and since Part 15 devices are not "licensed" nor were they specifically "authorized by or under" the Act at the time Section 333 was enacted, Congress could not reasonably have intended Section 333 to

---

9/ *See* Petition at 9.

10/ *See* 47 U.S.C. § 333.

11/ *See* H.R. Rep. 101-316, at 8-9 (Oct. 27, 1989) ("House Report") (for example, Congress intended Section 333 to "prohibit[] intentional jamming, deliberate transmission on top of the transmissions of authorized operators already using specific frequencies in order to obstruct their communications, repeated interruptions, and the use and transmission of . . . other types of noisemaking devices to interfere with the communications or radio signals of other stations."); *see also, e.g.*, *FCC Enforcement Advisory: Cell Jammers, GPS Jammers and Other Jamming Devices*, Public Notice, 26 FCC Rcd. 1329, 1329 (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.").

12/ *See* Petition at 4-5.

encompass Part 15 devices.[13] The Petitioners' argument is flawed. No radio transmissions are permitted under the Act unless they are licensed or permitted by rule.[14] While unlicensed users such as those operating under Part 15 do not receive a "license" in order to operate, their operations are clearly "authorized" by the FCC.[15] As the Commission has explained, "[w]hile we do not apply the term 'license' to the Part 15 approvals that are required to manufacture and distribute Part 15 devices, such approvals (*e.g.*, certifications for intentional radiators) constitute agency authorization for the manufacture, distribution and use of devices that have passed individualized requirements."[16] Accordingly, the Commission has explained that there is little to distinguish in a practical or legal sense Part 15 approvals of devices from traditional "licenses."[17]

The Petitioners also argue that because Part 15 was in existence at the time Section 333 was adopted and the statute's legislative history is devoid of any mention of either Part 15 operations or devices, Congress did not intend Section 333 to apply to "malicious interference" to Part 15 devices.[18] The fact that unlicensed devices were not listed in the legislative history of Section 333, however, is not meaningful. While the legislative history does not specifically

---

13/ *See* Petition at 5, 15.

14/ *See* 47 U.S.C. § 307 (stating that the FCC may either grant a license or authorize the operation of radio stations without individual licenses); *1998 Biennial Regulatory Review – 47 C.F.R. Part 90 – Private Land Mobile Radio Services,* Memorandum Opinion and Order and Second Report and Order, 17 FCC Rcd. 9830, ¶ 6, n.11 (2002) ("Instead of requiring radio stations to be licensed, the Commission may by rule authorize operation in certain radio services without individual licenses.") (citing 47 U.S.C. § 307(e)(1)).

15/ *See, e.g.*, *Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, Notice of Proposed Rulemaking and Order, 27 FCC Rcd. 15594, ¶ 38 (2012) ("*3.5 GHz Order*") ("Part 15 of the Commission's rules authorize unlicensed use of the spectrum, which allows for a great diversity of uses within any given band.").

16/ *Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems*, Second Report and Order and Second Memorandum Opinion and Order, 19 FCC Rcd. 24558, ¶ 75 (2004).

17/ *See id.*

18/ *See* Petition at 5, 15.

mention unlicensed services, it also does not mention the need to protect consumer wireless devices like smartphones from malicious interference. Nonetheless, as the Petitioners themselves recognize, these types of devices clearly fall under the protections of Section 333.[19] Moreover, Part 15 was in existence at the time Section 333 was adopted. If Congress wished to exclude Part 15 devices from Section 333, it could have done so explicitly. However, it did not.

The Petitioners also contend that extension of Section 333 to apply to interference to Part 15 devices would lead to illogical consequences, such as a finding that a homeowner's use of her cordless phone in a manner that interferes with a neighbor's phone and that a housewife's use of a baby monitor that interferes with a neighbor's garage door opener violate federal law.[20] Contrary to the Petitioners' parade of horribles, application of Section 333 to malicious interference with Part 15 communications would not lead to such absurd conclusions. The plain language of the statute states that Section 333 prohibits *willful and malicious* interference to communications. Interference resulting merely from Part 15 compliant devices transmitting on the same frequency under normal operating conditions would not be construed as being willful or malicious.

B. Blanket De-Authentication is Contrary to the FCC's Rules

In addition to being contrary to the Act, the de-authentication function the Petitioners describe violates the Commission's rules. As the Petitioners concede, Part 15 users operate on equal footing – they are all prohibited from causing harmful interference and must accept interference from one another.[21] The very architecture of Wi-Fi networks and other unlicensed applications requires that they share spectrum with each other – working to mutually minimize

---

19/ *See* Petition at 13-14.

20/ *See* Petition at 17.

21/ *See* Petition at 16; 47 C.F.R. § 15.5(b).

interference – while not causing harmful interference to licensed spectrum users.[22] By authorizing the use of unlicensed spectrum in this way, the Commission has devised a policy that sparks the development of innovative devices and applications that the wireless industry supports for expanding access to mobile broadband services. The Petitioners nonetheless propose that the FCC authorize one Part 15 user to purposefully shut down another Part 15 user through de-authentication in order to provide a better user experience. This would, in effect, make one Part 15 user the primary user of all unlicensed frequencies, contrary to the basic principles of Part 15 operations. Similarly, allowing an entity to "manage" the Part 15 spectrum ecosystem, by determining who could access unlicensed spectrum and who could not, would make that entity a Part 15 "czar," a concept inconsistent with Part 15 principles.

The Petitioners suggest that, because the FCC's rules require Part 15 devices to "accept whatever interference is received," they cannot be protected from interference under Section 333 of the Act.23 This interpretation of the FCC's rules, however, is flawed. Petitioners confuse interference with other Part 15 "devices" with "interference with communications," which is specifically addressed by Section 333. The FCC's requirement that a Part 15 operator "accept interference" extends only to the usual transmissions from other Part 15 devices, not to a targeted attempt to de-authenticate.

III. BLANKET DE-AUTHENTICATION IS CONTRARY TO PUBLIC POLICY

The public interest supports the foregoing interpretations of Section 333 of the Act and Part 15 of the FCC's rules. As noted above and recognized by the Commission, Wi-Fi plays a

---

22/ Sharing in the unlicensed bands is based on protocols that have emerged from an industry-driven standards process (*i.e.*, a set of steps and protocols that a device must follow before it may access the spectrum). *See, e.g.*, *Modification of Parts 2 and 15 of the Commission's Rules for Unlicensed Devices and Equipment Approval*, Order and Second Memorandum Opinion and Order, 29 FCC Rcd. 6366 (2014) ("*Spectrum Etiquette Order*").

23/ *See* Petition at 16-17.

valuable role in the wireless ecosystem and is an important tool through which CTIA members promote greater access to broadband connectivity.[24] The rapid growth of mobile data traffic has incentivized service providers to "find means, potentially intermodal, to reduce congestion on their mobile wireless networks,"[25] making both licensed and unlicensed spectrum important and complementary assets for providers.[26] In fact, Cisco reported earlier this year that 45 percent of global mobile data traffic was offloaded onto the fixed network through Wi-Fi or femtocells in 2013 and that, by 2018, there will be more traffic offloaded from cellular networks onto Wi-Fi than remain on cellular networks.[27] Without offloading, mobile data traffic is predicted to have grown 98 percent – rather than 81 percent – in 2013.[28]

24/ *See 3.5 GHz Order* ¶ 39 (noting that commercial adoption of standards such as Wi-Fi and the use of unlicensed spectrum bands "have become increasingly important for mobile broadband data capacity and coverage over the past several years"); *see also Marriott Order* ¶ 2 ("Wi-Fi is an essential on-ramp to the Internet.").

25/ *Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993; Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Including Commercial Mobile Services*, Sixteenth Report, 28 FCC Rcd. 3700, ¶ 373 (2013) ("*Sixteenth Wireless Competition Report*").

26/ *See, e.g.*, *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment*, Second Report and Order and Third Further Notice of Proposed Rulemaking, 29 FCC Rcd. 9846, ¶ 125 (2014) ("*Text-to-911 Third FNPRM*") (noting that CMRS providers migrating to 4G LTE networks "have network traffic and engineering incentives to off-load their subscriber traffic on to Wi-Fi networks that are connected to wired broadband connections"); *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, First Report and Order, 29 FCC Rcd. 4127, at Statement of Chairman Tom Wheeler (2014) (stating that today, "licensed and unlicensed spectrum are more complimentary then competitive"); *Sixteenth Wireless Competition Report* ¶ 373; *see also* CTIA Spectrum White Paper Comments at 15.

27/ *See Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018*, Cisco, at 2-3, 17-18 (Feb. 5, 2014) ("*Cisco 2014 VNI*"), *available at* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf; *see also Assessment of the Future Economic Value of Unlicensed Spectrum in the United States*, Telecom Advisory Services, LLC, at 9 (Aug. 2014), *available at* http://www.wififorward.org/wp-content/uploads/2014/01/Katz-Future-Value-Unlicensed-Spectrum-final-version-1.pdf (reporting that Wi-Fi cellular offloading traffic is growing at 68 percent per year).

28/ *Cisco 2014 VNI* at 2.

Because Wi-Fi offloading eases congestion on licensed spectrum bands,[29] most carriers make available or support personal MiFi and similar devices that operate in connection with carrier networks using licensed spectrum.[30] Through the use of devices, applications, and techniques like these that operate in connection with licensed networks, more American businesses and consumers are being provided access to mobile broadband, which result in everything from everyday conveniences and efficiencies to important public safety applications[31] to the next innovation in the Internet of Things. De-authentication, however, would interfere with these efforts by wireless carriers to manage the flow of traffic on their licensed spectrum bands and increase the strain on licensed spectrum generally, thereby thwarting valuable public interest benefits that can be attained. Conversely, multiple Wi-Fi networks offer multiple

---

29/ *See, e.g.*, *Connecting America: The National Broadband Plan*, at 95 (2010) ("*National Broadband Plan*"), *available at* http://www.broadband.gov/plan/ (stating that, "with the availability of Wi-Fi networks in many locations that enable users to take much of their data off of a licensed network, users benefit by obtaining much faster service while licensed providers have less congestion and can deliver a better overall quality of service"); *Mobile Broadband Explosion, The 3GPP Wireless Evolution*, 4G Americas, at 11-12 (2012), *available at* http://www.4gamericas.org/documents/4G%20Americas%20Mobile%20Broadband%20Explosion%20August%2020121.pdf (stating that Wi-Fi networks provide a means for offloading heavy traffic from LTE networks as the number of Wi-Fi hotspots increases, adding capacity by using unlicensed spectrum, and achieving high frequency re-use); Richard Thanki, *The Economic Significance of License-Exempt Spectrum to the Future of the Internet*, at 36-40 (June 2012), *available at* http://download.microsoft.com/download/A/6/1/A61A8BE8-FD55-480B-A06F-F8AC65479C58/Economic%20Impact%20of%20License%20Exempt%20Spectrum%20-%20Richard%20Thanki.pdf (stating that, in the absence of Wi-Fi offloading, wireless carriers would be forced to carry more traffic on their networks, which would result in increased costs that would be borne by consumers).

30/ *See, e.g.*, AT&T News Release, *AT&T Announces Company's First MiFi Intelligent Mobile Hotspot* (Nov. 17, 2010), *available at* http://www.att.com/gen/press-room?pid=18772&cdvn=news&newsarticleid=31372; *MiFi Hotspot – Explore Mobile Hotspots*, Verizon Wireless (last visited Dec. 14, 2014), http://www.verizonwireless.com/wcms/consumer/explore/mobile-hotspots.html; *Samsung 4G LTE Mobile Hotspot Pro | Mobile Hotspots*, T-Mobile (last visited Dec. 14, 2014), http://www.t-mobile.com/internet-devices/samsung-lte-mobile-hotspot-pro.html.

31/ *See, e.g.*, *Text-to-911 Third FNPRM* ¶ 125 (noting that the public interest warrants further exploration of the feasibility of sending 911 text messages over non-Commercial Mobile Radio Service ("CMRS") networks); *National Broadband Plan* at 95 (discussing the innovative applications and devices that have been made possible by the use of unlicensed spectrum).

options for broadband connectivity. Thus, the public is best served by increasing the potential for these networks, not allowing an individual Wi-Fi network manager unilaterally to shut them down.

IV. WI-FI OPERATORS HAVE OTHER MEANS TO MANAGE THEIR NETWORKS

Preventing Wi-Fi operators from de-authenticating on a blanket basis will not affect their ability to manage their networks. Wi-Fi network operators can continue to allow or disallow access to their networks for any particular device or user.[32] These techniques may be effective against the very threats that the Petitioners describe. Network operators also may use other methods to manage their networks. For instance, Wi-Fi operators can deny port access or use MAC address blacklists to protect Wi-Fi networks from "honeypot" or other security threats. Additionally, as the Petitioners and the Commission have recognized, operators can tune devices to less congested frequencies or hop to a number of different frequencies to avoid interference, or reduce the separation distance between the transmitter and receiver.[33] Each of these options, which do not involve disabling third-party access points, would be well within the network operator's authority to manage its own network and promote a better user experience without affecting third-party operators' ability to manage theirs.

V. CONCLUSION

While CTIA appreciates Wi-Fi operators' needs to protect their networks from harmful attacks, the Petitioners' request goes too far. Grant of the Petition would give such operators

---

32/ *See* Petition at 8-10 (discussing the use of FCC-authorized network management systems that mitigate security threats from unauthorized access points). By way of a more extreme example, the Petitioners also suggest that hotels might decide to "prohibit guests from bringing Part 15 devices on the hotel's property" or "limit the areas where Part 15 devices may be used" as a means of ensuring the reliability and security of their networks. *See* Petition at 21.

33/ *See* Petition at 12; *Spectrum Etiquette Order* ¶ 10.

broad authority to de-authenticate and shut down any and all Part 15 devices, including mobile devices that utilize Part 15 frequencies, in contravention of the Act, the FCC's rules, and public policy. CTIA therefore respectfully requests that the Commission prohibit this type of blanket policing activity and declare that it constitutes a violation of Section 333 of the Act and Part 15 of the FCC's rules.

Respectfully submitted,

*/s/ Brian M. Josef*_____
Brian M. Josef
Assistant Vice President, Regulatory Affairs

Scott K. Bergmann
Vice President, Regulatory Affairs

Michael F. Altschul
Senior Vice President & General Counsel

CTIA – The Wireless Association®
1400 16th Street, N.W., Suite 600
Washington, D.C. 20036
(202) 785-0081

December 19, 2014

CERTIFICATE OF SERVICE

I, Brian M. Josef, do hereby certify that on this 19th day of December, 2014, I caused a copy of the foregoing Comments of CTIA–The Wireless Association®, to be served by first class mail and email on the following:

Bennett L. Ross
David Hilliard
Henry Gola
Wiley Rein LLP
1776 K Street, NW
Washington, DC 20006
(202) 719-7000
bross@wileyrein.com
Counsel for Marriott International, Inc. and Ryman Hospitality Properties

Banks Brown
McDermott Will & Emery LLP
340 Madison Avenue
New York, NY 10173-1922
(212) 547-5488
bbrown@mwe.com
Counsel for the American Hospitality & Lodging Association

/s/ Brian M. Josef