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-11737

REPLY COMMENTS IN SUPPORT OF PETITION FOR DECLARATORY RULING OR, IN THE ALTERNATIVE, FOR RULEMAKING

Banks Brown
McDermott Will & Emery LLP
340 Madison Avenue
New York, NY 10173-1922
212 547 5488

Counsel for the American Hotel & Lodging Association

Bennett L. Ross
David E. Hilliard
Henry Gola
Wiley Rein LLP
1750 K Street, NW
Washington, DC 20006
(202) 719-7000

Counsel for Marriott International, Inc. and Ryman Hospitality Properties

January 5, 2015

TABLE OF CONTENTS

PAGE

I. INTRODUCTION AND SUMMARY 1

II. ARGUMENT 9

- A. The Relief Petitioners Seek Is Narrowly Limited, Notwithstanding Claims By Several Commenters To The Contrary 9
- B. The Commission Has Never Previously Interpreted Section 333 To Apply To Part 15 Devices. 11
- C. Section 333 Cannot Lawfully Be Read To Apply To Part 15 Devices. 16
- D. Interpreting Section 333 To Apply To Part 15 Devices Would Lead To Illogical Results. 24
- E. Granting The Petition Would Not Harm Consumers Or Otherwise Adversely Affect The Commission's Part 15 Regime. 26
- F. Commenters Opposing The Petition Misconstrue The Significance of the Commission's Equipment Authorization and OTARD Rules. 29

III. CONCLUSION 32

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-11737

REPLY COMMENTS IN SUPPORT OF PETITION FOR DECLARATORY RULING OR, IN THE ALTERNATIVE, FOR RULEMAKING

I. INTRODUCTION AND SUMMARY

The Commission should grant the petition by the American Hotel & Lodging Association ("AH&LA"), Marriott International, Inc., and Ryman Hospitality Properties (collectively, "Petitioners") seeking a declaratory ruling or, in the alternative, a rulemaking to address the circumstances under which a Wi-Fi operator may lawfully use FCC-authorized equipment in managing its network and protecting its guests without violating 47 U.S.C. § 333 ("Petition").

Numerous commenters support the Petition, including enterprise users,[1] equipment providers,[2] trade associations,[3] and network operators.[4] These commenters generally agree that

---

[1] Statement of Ad Hoc Telecommunications Users Committee in Support of Petition for Declaratory Ruling or, in the Alternative, for Rulemaking, RM-11737, at 1 (filed Dec. 19, 2014) ("Ad Hoc Statement").

[2] Comments of Cisco System, Inc., RM-11737, at 4-5 (filed Dec. 19, 2014) (supporting issuance of "a policy statement on the network management issues" but opposing "a rulemaking at this time"); Joint Comments of Aruba Networks, Inc. and Ruckus Wireless, Inc., RM-11737, at 2 (filed Dec. 19, 2014) ("Joint Comments").

[3] Comments of the Enterprise Wireless Alliance, RM-11737, at 1-2 (filed Dec. 19, 2014) ("EWA Comments"); Comments of the United States Telecom Association, RM-11737, at 1 (filed Dec. 22, 2014) ("USTelecom Comments").

Section 333 does not apply to Part 15 devices. By the same token, they acknowledge the uncertainty regarding the extent to which a Wi-Fi operator can take reasonable steps to protect the security and reliability of its Wi-Fi service and to safeguard its guests – uncertainty that the Commission can and should resolve.[5] There also is general agreement that these issues affect not only the hospitality industry but every Wi-Fi network operator, which underscores the need for uniform standards applicable to all Wi-Fi networks.[6]

At the outset, claims that Petitioners are seeking a "carte blanche" or "virtually boundless" "right to interfere" with their guests' use of personal Wi-Fi hot spots are not true.[7] The Petition seeks guidance from the Commission on the extent to which Wi-Fi operators can engage in reasonable measures to ensure secure and reliable Wi-Fi service on their property using FCC-authorized equipment. It would be unreasonable – and inconsistent with the relief sought in the Petition – for a Wi-Fi operator to prevent a person from making use of a personal

---

(footnote cont'd.)

[4] Comments of Hilton Worldwide Holdings Inc. in Support of American Hotel & Lodging Association Petition for Declaratory Ruling or, in the Alternative, for Rulemaking, RM-11737, at 1 (filed Dec. 19, 2104) ("Hilton Comments"); Comments of Smart City Networks, LP, RM-11737, at 1 (filed Dec. 19, 2014) ("Smart City Comments").

[5] *See, e.g.,* Ad Hoc Statement at 2 (urging "the Commission to develop a robust factual record on the basis on which it can then establish clear, generally applicable standards and policies"); EWA Comments at 2 (recommending that the Commission adopt rules "for the benefit of Wi-Fi network operators and consumers"); Cisco Comments at 21 (urging the Commission to issue a policy statement on Wi-Fi management "that identifies and recommends the use of industry best practices promoting the use of the unlicensed spectrum in accordance with evolving public policy objectives and discouraging questionable conduct").

[6] *See* Ad Hoc Statement at 1-2; USTelecom Comments at 3-4; EWA Comments at 2-3.

[7] Opposition of the Wireless Internet Service Providers Association to Petition for Declaratory Ruling or, in the Alternative, for Rulemaking, RM-11737, at 3 (filed Dec. 19, 2014) ("WISPA Opposition"); Opposition of Open Technology Institute at New America Foundation ("OTI") and Public Knowledge ("PK") to Petition for Declaratory Ruling or, in the Alternative, for Rulemaking, RM-11737, at 2 (filed Dec. 19, 2014) ("OTI/PK Opposition").

Wi-Fi hot spot when such use does not threaten the security or reliability of the Wi-Fi operator's network or pose a risk to its guests.

Equally untrue are claims that the Petition seeks to authorize hotels to disable personal Wi-Fi hot spots in order to force guests to purchase Wi-Fi service from the hotel where they are staying or visiting.[8] There is no evidence that hotels are engaging or have engaged in such a tactic, which, in any event, would not constitute a reasonable measure to ensure a safe and reliable Wi-Fi service.[9] Indeed, as far as Petitioners are aware, overnight guests at AH&LA member hotels can use personal Wi-Fi hot spots in their rooms without any fear that the hotel will "disable" their devices.

To the extent a hotel has installed FCC-authorized equipment to monitor and manage its Wi-Fi network, such equipment is generally only used in meeting rooms, convention centers, and other high-density areas where the threat to security and reliability is the greatest. And, a guest using a smartphone or Mi-Fi device as a personal Wi-Fi hot spot is rarely going to pose such a threat or be subject to the deauthentication process that is at issue in this proceeding. Rather, deauthentication is typically used only to address the problems posed by a person or company that sets up a Wi-Fi service on a hotel's private property that is offered to other visitors and that jeopardizes the reliability or security of the hotel's Wi-Fi service. In short, the scope of the Petition is considerably more narrow than some commenters suggest.

Every commenter agrees about the importance of Wi-Fi and its increasing prominence as a method of Internet access. But commenters fundamentally disagree about whether Section 333 prohibits a Wi-Fi operator's use of FCC-authorized to deauthenticate an access point that threatens the security or reliability of its network or poses a risk to its guests. Given the lack of

---

8 *See, e.g.*, OTI/PK Opposition at 3 & 11.

9 *See* Hilton Comments at 5.

clarity in this area, and the public interest in safe and reliable Wi-Fi service, the Commission should grant the Petition in order to provide guidance on these issues.

Regardless of the procedural vehicle, the Commission's guidance is particularly appropriate given the federal government's emphasis on cybersecurity – reinforced by enforcement actions by both the FCC and the Federal Trade Commission – and with the catastrophic consequences for a business that may fall victim to a cyber-attack (most recently, Sony).[10] Absent Commission leadership, a Wi-Fi operator proceeds at its peril when deauthenticating a Part 15 device being operated on its premises that poses a risk to the security of its guests or network. As one commenter correctly observes, Wi-Fi operators should not have to confront a "regulatory Hobson's choice" of risking an enforcement action for failing to mitigate the security threat posed by an unauthorized access point on the one hand or risking an enforcement action for deauthenticating that access point in order to protect its guests or its network on the other hand.[11]

The risk is particularly acute for commercial enterprises – such as hotels – that serve a quasi-public purpose. Such enterprises owe a duty of care with respect to their guests, including a duty to take reasonable steps to prevent their premises from becoming a place where criminal activity occurs. For hotels, with millions of guests staying overnight and with hundreds of thousands of groups booking meetings and conventions annually, the Petition seeks guidance on

---

[10] *See Terracom, Inc. & Yourtel Am., Inc.*, Notice of Apparent Liability for Forfeiture, FCC 14-173 (rel. Oct. 24, 2014); Complaint of the Federal Trade Commission, *FTC v. Wyndham Worldwide Corp.*, No. CIV.A. 13-1887 (June 26, 2012); *see also* Ted Johnson, "Sony Hit With Fourth Class Action Lawsuit Over Hacking Attack," *Variety* (Dec. 19, 2014) (noting latest class action brought against Sony by former employees challenging the measures taken by the studio to protect employee personal information), available at http://variety.com/2014/biz/news/sony-hit-with-fourth-class-action-lawsuit-over-hacking-attack-1201383743/.

[11] Hilton Comments at 11-14; *see also* USTelecom Comments at 1-2.

the steps that a Wi-Fi operator can legally take to provide a secure and reliable Wi-Fi service for customers who demand and expect that their personal information will remain private.

In opposing the Petition, some commenters contend that neither a declaratory ruling nor a rulemaking is necessary because resolution of the issues raised by Petitioners is "clear."[12] However, the diversity of comments in this proceeding establish otherwise.[13]

To further understand the differing interpretations and regulatory uncertainty in this area, the Commission need look no further than the following situation referenced in the Petition that is a common method employed by bad actors: a person visiting a hotel sets up an access point in a meeting room or convention center and launches a spoofing (or "honey pot") attack by advertising a service set identifier ("SSID") purporting to be that of the hotel's Wi-Fi network in an attempt to obtain credit card or other personal information of hotel guests. Even in this narrow situation, commenters cannot agree on whether a hotel violates Section 333 by deauthenticating this access point utilizing FCC-authorized equipment in an effort to protect its guests.

In fact, there is no agreement on threshold issues, such as whether deauthentication, which is part of the IEEE 802.11standard, even constitutes "interference" within the meaning of

---

12 *See* OTI/PK Opposition at 1; Comments of Microsoft Corp., RM-11737, at 1 (filed Dec. 19, 2014) ("Microsoft Comments"); *see also* Opposition of the National Cable & Telecommunications Association ("NCTA Opposition"), RM-11737, at 2 (filed Dec. 19, 2014) ("NCTA Opposition"); Opposition of Google, Inc., RM-11737, at 1 (filed Dec. 19, 2104) ("Google Opposition").

13 While disagreeing with the relief requested in the Petition, both CTIA and the Wireless Internet Service Providers Association ("WISPA") seek declaratory rulings of their own. *See* Comments of CTIA–The Wireless Association®, RM-11737, at 4 (filed Dec. 19, 2014) ("CTIA Comments") ("The Commission should declare that the type of de-authentication described by the Petition is prohibited by Section 333 of the Act"); WISPA Opposition at 14.

Section 333 or whether an access point is even a "station" protected under Section 333.[14] Based on their view of these issues, many commenters assert that there would be no Section 333 violation.[15] While recognizing that security is a genuine concern, other commenters insist that the hotel would violate Section 333 in this scenario because the statute prohibits any "willful interference," even for wholly laudable purposes including protecting a hotel's guests from a cyber-attack.[16] By contrast, WISPA and NCTA – while opposing the Petition – nonetheless believe that Section 333 would not prohibit the hotel from deauthenticating the unauthorized access point if it was connected to the operator's network.[17] CTIA has a different view; while agreeing that Wi-Fi operators have legitimate needs to protect against malicious interference, it argues that any use of a deauthentication feature under any circumstances is unlawful.[18] That no

---

14 *Compare* Cisco Comments at 14-16 *with* Microsoft Comments at 4.

15 *See, e.g.,* Hilton Comments at 8-9; Cisco Comments at 19-21; Joint Comments at 6-10; Smart City Comments at 7-11.

16 OTI/PK Opposition at 10 ("Unfortunately for Petitioners, there is neither a self-defense nor quality of service (QoS) 'right to cause interference' exception in either Section 333 or in the Part 15 rules"); *see id.* at 13, n.36 (a Wi-Fi operator has no legal authority to "not authorize radio communications within its venue or anywhere else"); Microsoft Comments at 6-7.

17 WISPA Comments at 14; NCTA Opposition at 14-15. WISPA's "solution" to the spoofing scenario – that it be "shut down with the assistance of law enforcement" – is no solution at all, given the inevitable delay that would result in involving law enforcement personnel and the inherent challenges in physically locating the perpetrator in a crowded hotel. WISPA Comments at 14.

18 CTIA Comments at 2-3. CTIA argues that Wi-Fi operators have other means besides deauthentication to protect their networks by, for example, denying "port access" or using "MAC address blacklists to protect Wi-Fi networks from 'honeypot' or other security threats." CTIA Comments at 10. However, denying port access or blacklisting would only prevent unauthorized access to the Wi-Fi operator's network and, in the case of blacklisting, requires that the Wi-Fi operator know the MAC address of the offending device. Thus, neither technique would protect users when an intruder is spoofing the SSID of the hotel's Wi-Fi network. Furthermore, for at least some of the network management equipment at issue in this proceeding, blacklisting involves the transmittal of deauthentication packets "to force the client to disconnect." http://www.arubanetworks.com/techdocs/ArubaOS_61/ArubaOS_61_UG/New_WIP.php#XREF_54583_Client_Blacklisting.

common understanding exists regarding the scope of Section 333 confirms the need for the Commission to issue a declaratory ruling resolving these issues.[19]

Alternatively, the Commission should initiate a rulemaking to "establish clear standards for the industry to follow" in the management of Wi-Fi networks.[20] While Wi-Fi is increasingly important to consumers in accessing the Internet, the lack of regulatory clarity may prevent the benefits of Wi-Fi from being fully realized.

Assertions by some commenters that the Petition should be denied because the Commission previously has interpreted Section 333 to apply to Part 15 devices are without merit. In fact, the *Commission* has never addressed the issues raised in the Petition. Although the *Enforcement Bureau* has issued several advisories about "jammers," only one of which actually mentions Section 333, these advisories are not legally controlling because: (i) their reasoning has never been affirmed by the Commission; (ii) they represent at most bureau-level policy statements, which are not binding on the agency; and (iii) the equipment at issue are not "jammers" but rather are FCC-authorized network management tools. The Petition presents the

---

19 *See, e.g., NARUC Petition for Clarification or Declaratory Ruling*, Memorandum Opinion and Order, 25 FCC Rcd 5051 (2010) (granting declaratory ruling when "[t]he record reflects widespread uncertainty regarding whether the Commission has preempted the States from mandating the filing of broadband information"); *Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service*, Memorandum Opinion and Order, 19 FCC Rcd 3307, n.24 (2004) ("Based on the record in this proceeding and in accordance with our rules, it is evident that there is sufficient uncertainty about the classification of Pulver's service offering to warrant a declaratory ruling"); *In re Southwestern Bell Mobile Sys., Inc.*, Memorandum Opinion and Order, 14 FCC Rcd 19898, ¶ 5 (1999) (agreeing to issue declaratory ruling when there was "substantial uncertainty whether and to what extent" pending class action lawsuits were precluded by the Communications Act, as evidenced – in part – by "extensive comments ... filed by interested parties").

20 *See Rechannelization of the 17.7-19.7 GHz Frequency Band for Fixed Microwave Services under Part 101 of the Commission's Rules*, Notice of Proposed Rulemaking, 19 FCC Rcd 7260, ¶ 14 (2004).

first opportunity to resolve whether Section 333 applies to Part 15 devices – an opportunity the Commission should seize.

In construing the scope of the statute, the Commission should find that the transmission of deauthentication packets to a Part 15 device does not involve "interference" to a "station … authorized by or under this chapter" within the meaning of Section 333. Such a finding would comport with the plain language of the statute and its legislative history, would avoid conflicts with other provisions of the Act, and would be consistent with the Part 15 regime. That Section 333 does not apply to Part 15 devices would not preclude the Commission from adopting rules or otherwise providing guidance on the reasonable measures that a Wi-Fi operator can employ in ensuring secure and reliable Wi-Fi service on its property. The Commission plainly has such authority, as all commenters agree.

In addition to being unsupported by the plain language of Section 333 and the statute's legislative history, any interpretation of Section 333 to prohibit "willful interference" to Part 15 devices would lead to illogical results. It would effectively put the user of any Part 15 device in the enforcement crosshairs when the knowing operation of that device results in interference to another Part 15 device. Commenters who claim otherwise rely upon a flawed and unsupported definition of "willful," which they mistakenly insist requires bad faith or an evil purpose. As defined under the Act and interpreted by the Commission, "willful" only requires a voluntary act – that is, the act was not accidental. Thus, "willful" is a very low threshold that almost any interference to a Part 15 device is likely to meet.

Granting a declaratory ruling or initiating a rulemaking would not create a property interest in spectrum, threaten the public safety, or jeopardize innocent bystanders, as some commenters contend in opposing the Petition. On the contrary, the Commission can protect

these various interests by resolving the issues in the Petition rather than accepting the invitation of some commenters to ignore them.

Finally, the Commission must rationalize its interpretation of Section 333 with its equipment authorization and Over-the-Air Reception Devices ("OTARD") rules to ensure regulatory consistency. That the network equipment at issue has been authorized by the Commission means that it is not the equivalent of a jammer and can be operated without causing "harmful interference" prohibited by Part 15. Under the circumstances, it would be beyond strange for the Commission to find that the operation of the equipment it has expressly authorized nonetheless causes "interference" prohibited by Section 333. Likewise, OTARD prohibits any "restriction" on the "use" of a Wi-Fi device, but this prohibition only applies if the operator of that device has a sufficient "ownership or leasehold" interest in the property where the device is located. Because hotel guests lack any "ownership or leasehold" interest in a hotel's property, the Commission should consider whether applying Section 333 to Part 15 devices would effectively extend OTARD beyond the limited group of owners or lessees the OTARD rules are intended to protect.

II. ARGUMENT

A. <u>The Relief Petitioners Seek Is Narrowly Limited, Notwithstanding Claims By Several Commenters To The Contrary.</u>

Several commenters mischaracterize the relief Petitioners are seeking. For example, WISPA asserts that the Petition asks for a "carte blanche 'right to interfere,'"[21] while OTI/PK

---

21 WISPA Opposition at 3.

insist that Petitioners are seeking a "'right to interfere' with Wi-Fi or other Part 15 operations" that is "virtually boundless."[22]

Nothing could be further from the truth. The Petition requests clarification that Section 333 does not apply to Part 15 devices and that a Wi-Fi network operator is permitted to take reasonable steps to provide a secure and reliable Wi-Fi service using FCC-authorized equipment. Thus, the lynchpin of the Petition – and a plain limitation on any activity in which a Wi-Fi operator may engage – is whether those activities are reasonably necessary to ensure Wi-Fi security and reliability.

That the requested relief is limited to reasonable measures in providing a secure and reliable Wi-Fi service should alleviate commenter concerns about the alleged breadth of the Petition or the purported negative effects of granting such relief. For example, it certainly would not be reasonable for Wi-Fi operators "to intentionally interfere with the devices of their customers, guests, and others, *for any reason they deem fit*."[23]

The same is true for "economically-motivated interference" by which a Wi-Fi operator allegedly seeks to "disabl[e] competing options and rival Wi-Fi services" in an attempt to "coerce guests and visitors to pay them" for Wi-Fi connectivity that they are buying from someone else.[24] There is no evidence that hotels are using or have used deauthentication in an attempt to force guests to purchase their Wi-Fi services. In fact, the record establishes

---

22 OTI/PK Opposition at 2; *see also* NCTA Opposition at 1 (alleging that Petitioners seek a right to disrupt any Wi-Fi signal of anyone who "behaves in a manner inconsistent with the owner's business objectives").

23 WISPA Opposition at 12 (emphasis added); *see also* CTIA Comments at 1 (urging the Commission to "deny Petitioners' request to give network operators blanket authority to shut down any and all Part 15 devices").

24 OTI/PK Opposition at 3 & 11; *see also* Google Opposition at 1; Microsoft Comments at 7.

otherwise.[25] In short, the Commission can readily distinguish between reasonable practices and unreasonable conduct in establishing standards that would apply to all network operators in offering Wi-Fi service.

B. The Commission Has Never Previously Interpreted Section 333 To Apply To Part 15 Devices.

In opposing the Petition, certain commenters erroneously assert that the Commission has previously "interpreted Section 333 to prohibit interference to Part 15 devices" and has "found a violation of Section 333 based upon such interference."[26] But these commenters do not and cannot point to a single *Commission* decision in support of this assertion. Instead, they rely upon a series of advisories by the Enforcement Bureau about jammers[27] and a recent consent decree[28] that have no legal effect or precedential significance.

---

[25] *See* Hilton Comments at 5 ("Hilton is not seeking to use reasonable network management techniques as a pretext to compel guests to purchase Wi-Fi services from Hilton when visiting one of its hotels").

[26] WISPA Comments at 3-4; *see also* Google Opposition at 5 ("The Commission has consistently prohibited willful interference to Part 15 communications"); OTI/PK Opposition at 4 (claiming that the FCC "has a longstanding policy that willful interference to any authorized radio service, including Wi-Fi operations, violates federal law"); Microsoft Comments at 5 ("The Commission has made clear on numerous occasions that intentional interference with unlicensed devices violates Section 333").

[27] FCC Enforcement Advisory: Cell Jammers, GPS Jammers, and Other Jamming Devices, Enforcement Advisory No. 2011-04, Public Notice, 26 FCC Rcd. 1329, 1 (Enf. Bur. 2011) ("2011 Advisory"); FCC Enforcement Advisory: Cell Jammers, GPS Jammers, and Other Jamming Devices, Enforcement Advisory No. 2012-02, Public Notice, 27 FCC Rcd. 2309, 2 (Enf. Bur. 2012); FCC Enforcement Advisory: Jammer Use is Prohibited, Enforcement Advisory No. 2014-05, Public Notice, DA 14-1785, 1 (Enf. Bur., Dec. 8, 2014).

[28] *Marriott International, Inc., Marriott Hotel Services, Inc.*, File No. EB-IHD-13-00011303, Acct. No. 201532080001, FRN 0022507859, FRN, 0006183511, Order, 29 FCC Rcd 11760 (Enf. Bur. 2014). This consent decree does not contain any admission of liability and expressly provides that it "does not constitute either an adjudication on the merits or a factual or legal finding or determination regarding any compliance or noncompliance with the Communications Laws." Under the circumstances, the claim by some commenters that this consent decree represents a "determination" or a "finding" by the Commission that Marriott violated Section 333 is inaccurate. *See* WISPA Opposition at 2; Google Opposition at 6.

First, Enforcement Bureau advisories are not legally controlling as their reasoning has never been affirmed by the Commission. In *Comcast Corp. v. FCC*, 526 F.3d 763, 769 (D.C. Cir. 2008), the D.C. Circuit embraced the "well-established view that an agency is not bound by the actions of its staff if the agency has not endorsed those actions." The Commission follows this same approach: "When decisions on an issue have been made solely at a subordinate level within the agency … the first case presented for decision to the agency's highest authority is a case of first impression, and any prior unchallenged staff decisions are not considered Commission precedent."[29] While bureau decisions have the force of law in the absence of Commission action, 47 U.S.C. § 155(c)(3), "this simply means that those rulings are binding on the parties to the proceeding .... [U]nchallenged staff decisions are not Commission precedent ...."[30]

Second, the Enforcement Bureau advisories do not even represent bureau-level decisions, as they were not the product of an agency proceeding. At most, they represent bureau-level policy statements. Under the Administrative Procedure Act ("APA"), a policy statement does not represent substantive law but rather only "indicates an agency's inclination or leaning, not in any way binding on the agency."[31] The APA distinguishes between "general statements of

---

[29] *In the Matter of T-Mobile USA, Inc., a subsidiary of T-Mobile US*, Inc., File No.EB-SED-13-00009310, Forfeiture Order, FCC 14-128 (rel. Aug. 27, 2014).

[30] *Comcast*, 526 F.3d at 770; *see also Cmty. Care Foundation v. Thompson*, 318 F.3d 219, 227 (D.C. Cir. 2003) ("There is no authority for the proposition that a lower component of a government agency may bind the decision making of the highest level"); *see also Jelks v. FCC*, 146 F.3d 878, 881 (D.C. Cir. 1998) (per curiam); *Amor Family Broad. Group v. FCC*, 918 F.2d 960, 962 (D.C. Cir. 1991).

[31] *Hudson v. Federal Aviation Administration*, 192 F.3d 1031 (D.C. Cir., 1999) (*citing Pacific Gas & Elec. Co. v. Federal Power Comm'n*, 506 F.2d 33, 38 (D.C. Cir. 1974); *United States Tel. Ass'n v. FCC*, 28 F.3d 1232, 1234 (D.C. Cir. 1994); *see also Brock v. Cathedral Bluffs Shale Oil Co.*, 796 F.2d 533 (D.C. Cir. 1986) (finding that the Secretary of Labor's enforcement guidelines under the Federal Mine Safety and Health Act were not binding on the agency).

policy" and "rules," and only the latter – which must comply with the APA's notice-and-comment rulemaking requirements – are legally enforceable.[32] As far as Petitioners are aware, none of the Enforcement Bureau advisories was published in the Federal Register or is contained in the Code of Federal Regulations, further demonstrating that they were not intended to, and cannot, have binding legal effect.[33]

Third, each of the Enforcement Bureau advisories is related to "jammers." Although some commenters attempt to obscure the significance of this fact, jammers cannot legally be used or sold in the United States. That obviously is not the case with the network management equipment at issue in this proceeding, which – in stark contrast to jammers – is extensively used by Wi-Fi operators, is widely available in the United States, and is authorized by the Commission. Nothing in any Enforcement Bureau advisory even remotely suggests that the use of FCC-authorized equipment to manage Wi-Fi networks is unlawful under Section 333.

Indeed, two of the Enforcement Bureau advisories upon which commenters rely in support of their view that the Commission has already resolved the issues in the Petition do not even mention Section 333. To be sure, the 2011 Advisory "remind[s] 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," citing Section 333.

---

32 *See, e.g.*, *Wilderness Soc'y v. Norton*, 434 F.3d 584, 597 (D.C. Cir. 2006) (denying claims based on document entitled "MANAGEMENT POLICIES" "because they are predicated on unenforceable agency statements of policy"); *Lutheran Church-Missouri Synod v. FCC*, 154 F.3d 487, 489 (D.C. Cir. 1998) ("a 'policy statement' . . . does not bind the Commission to a result in any particular case").

33 *See, e.g.*, *Brock*, 796 F.2d at 539 ("The real dividing point between regulations and general statements of policy is publication in the Code of Federal Regulations, which the statute authorizes to contain only documents 'having general applicability and legal effect,' . . . and which the governing regulations provide shall contain only 'each Federal regulation of general applicability and current or future effect.'") (citations omitted). Because the Enforcement Bureau advisories have no legally binding effect, they are not "entitled to deference," as Google contends. Google Opposition at 6.

However, because this reminder was offered in the context of jammers – which the 2011 Advisory also indicated "consumers cannot legally use … nor can retailers lawfully sell" – the passing reference to Wi-Fi was largely gratuitous. The 2011 Advisory certainly does not reflect "established, well-reasoned analysis" regarding whether Section 333 applies to Part 15 devices.[34] In fact, the Enforcement Bureau made no attempt in its one-page 2011 Advisory to grapple with any of these issues raised in the Petition or supporting comments.

The absence of guidance from the *Commission* on the application of Section 333 of Part 15 devices – as opposed to the views of the Enforcement Bureau – is the problem the Petition seeks to rectify. And the industry would plainly benefit from such guidance, as numerous commenters make clear.

Indeed, while opposing the Petition, WISPA concedes that some direction from the Commission would be helpful, expressly requesting that it "reaffirm" that a party may use Wi-Fi monitoring equipment "to manage its own network for reliability (*e.g.*, avoiding congestion) or to identify a legitimate security risk that poses a risk to users of its *own* network."[35] Likewise, NCTA asserts that Section 333 "does not limit a network operator's ability to manage its own network," which may include the "use of deauthentication packets or other techniques to disconnect a user from its own network …."[36]

However, the parameters of the circumstances under which WISPA and NCTA apparently would agree that network management by a Wi-Fi operator would not violate Section 333 are ill-defined and far from self-evident. For example, what steps, if any, can a Wi-Fi

---

34 *See* NCTA Opposition at 5.

35 WISPA Comments at 14 (emphasis in original). WISPA does not identify the prior Commission decisions addressing the ability of a Wi-Fi operator to manage its network in offering a reliable and secure service that it wants the Commission to "reaffirm."

36 NCTA Opposition at 14.

operator take to "manage its own network for reliability" without running afoul of Section 333 when such reliability is threatened by congestion in the airspace caused by other Wi-Fi devices being operated in a high-density area on the network operator's premises?[37] Likewise, can a Wi-Fi operator use network management equipment to mitigate a security risk to guests who are not actually using the operator's network but may erroneously believe they are because they are victims of a spoofing attack? And, when a Wi-Fi operator deauthenticates an unauthorized access point that also is physically connected to the operator's network for network security or reliability reasons, how is such conduct consistent with WISPA's and NCTA's interpretation of Section 333, which does not contain any exceptions to the statute's prohibition against "willful interference"?[38] Neither WISPA nor NCTA provides any insight into how these questions should be answered, which only reinforces the need for the Commission to grant the Petition.

---

[37] For example, in its *Open Internet Order*, the Commission found that "reducing or mitigating the effects of congestion on the network" is "a legitimate network management purpose" and noted that unlicensed spectrum poses "unique network management challenges," given that such "spectrum is shared among multiple users and technologies and no single user can control or assure access to the spectrum." *Preserving the Open Internet; Broadband Industry Practices*, Report and Order, 25 FCC Rcd 17905, ¶ 82 & ¶ 86 (2010) ("*Open Internet Order*"), *aff'd in part, vacated and remanded in part sub nom. Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

[38] NCTA insists that the use of deauthentication packets or other techniques to disconnect a user from the operator's own network would not constitute "interference" and would not be either "willful or malicious." NCTA Opposition at 14-15. Even though Petitioners agree that such use does not violate Section 333, NCTA's arguments provide cold comfort in the absence of any FCC rules, decisions, or other pronouncements on the subject. Indeed, nothing in Section 333 supports the distinction NCTA seeks to draw – *i.e.*, a network operator's deauthentication of a Wi-Fi hot spot connected to its network is permissible, while the deauthentication of a Wi-Fi hot spot not connected to its network violates Section 333.

C. Section 333 Cannot Lawfully Be Read To Apply To Part 15 Devices.

Certain commenters take issue with Petitioners' reading of Section 333.[39] In the process, however, some commenters misstate Petitioners' arguments. For example, OTI/PK's claim that Petitioners believe Section 333 protects "only 'licensed' services" is erroneous. Section 333, which is quoted in full in the Petition, plainly prohibits willful or malicious interference "to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government." The question is whether the transmission of deauthentication packets to a Part 15 device violates Section 333, and Petitioners – as well as other commenters – submit the answer is "no."

The comments filed in response to the Petition underscore basic disagreements regarding the proper interpretation of Section 333 – issues the Commission has never addressed. For example, commenters do not agree on whether the use of deauthentication packets to contain an unauthorized access point constitutes "interference" within the meaning of Section 333. As several commenters point out, deauthentication does not involve an increase in unwanted electromagnetic "energy," which is the interference Section 333 is designed to address; rather it entails "a standards-based exchange of network management information using defined protocols – protocols that the recipient interprets as a termination of its connection."[40]

---

39 OTI/PK Opposition at 6-9.

40 Joint Comments at 6-7; *see also* Cisco Comments at 13-16 (the transmission of "an IEEE 802.11 deauthentication frame to contain an AP or other device … does not cause electromagnetic interference"); Smart City Comments at 7 (deauthentication does not involve "the transmission of powerful radio signals to overpower, jam, or interfere with authorized communications").

Microsoft contends otherwise, asserting that the transmission of deauthentication packets falls within the meaning of "interference" as defined by the Commission.[41] However, because Section 333 prohibits all willful interference without exception, neither Microsoft nor any other commenter opposing the Petition explains how, under this interpretation, a network operator could lawfully use deauthentication techniques under any circumstances, even though deauthentication is "required by the 802.11 standard and necessary to the proper functioning of 802.11 compliant devices."[42]

Furthermore, construing deauthentication to constitute "interference" prohibited by Section 333 would have significant consequences from a cybersecurity standpoint. According to Smart City, the United States Department of Defense "mandates the use of network management and de-authentication technology in connection with its owned and operated networks," and the National Institute of Standards and Technology "has recommended the use of de-authentication technologies for all federal agencies and has provided guidance" governing such use.[43] Under the circumstances, other federal agencies are unlikely to embrace the view that any use of deauthentication constitutes impermissible "interference."[44]

Similarly, commenters disagree on whether a Part 15 device is a "radio station" under Section 333. As Cisco and others observe, the Commission historically has distinguished between "radio stations" or "stations" subject to various provisions of Title III (including

---

41 Microsoft Comments at 4 (quoting 47 C.F.R. § 2.1).

42 *See, e.g.,* Joint Comments at 8.

43 Smart City Comments at 2-3; *see also* Cisco Comments at 8.

44 That deauthentication is part of the 802.11 standard and is either mandated or recommended by various federal agencies renders unconvincing Google's theory that the use of deauthentication technology involves the transmission of "false or deceptive signals or communications" that would justify the suspension of an operator's license. Google Opposition at 4 (citing 47 U.S.C. § 303(m)(1)(D)(1).

applicable licensing requirements) and unlicensed devices.[45] By contrast, according to Microsoft, a Part 15 device is a "radio station" within the meaning of Section 333, because it is "a station equipped to engage in radio communication or radio transmission of energy" – a position apparently endorsed by NCTA.[46] However, neither Microsoft nor NCTA explains how, under their interpretation, a Part 15 "radio station" could be operated without the license called for in Section 307.[47]

Commenters also disagree about whether Part 15 devices are "licensed or authorized by or under this chapter" within the meaning of Section 333. With the exception of NCTA, no one contends that Part 15 devices are "licensed." This is not surprising, since, to state the obvious, unlicensed devices are not licensed by the Commission. The scope of Part 15 is explicit on this point: "This part sets out the regulations under which an intentional, unintentional, or incidental radiator may be operated *without an individual license*."[48]

NCTA's argument that FCC authorization of Part 15 equipment is akin to a "station license" is nonsensical.[49] Equipment authorizations are treated differently from and are subject to completely different regulatory requirements than radio station licenses. For example, equipment authorizations are not subject to Section 310(d), which requires prior Commission approval for the assignment or transfer of a "station license." Instead, a change in control of the holder of an equipment authorization requires only notification to the Commission after the

---

45 Cisco Comments at 16; *see also* Joint Comments at 9-10; Smart City Comments at 8-9.

46 Microsoft Comments at 4 (quoting 47 U.S.C. § 153(42)); NCTA Opposition at 10. NCTA erroneously claims that Petitioners "concede" that Part 15 devices "constitute a station authorized under the Communications Act." NCTA Opposition at 5. The Petition contains no such concession.

47 *See* Cisco Comments at 16-17; *see also* Joint Comments at 9-10.

48 47 C.F.R. § 15.1(a) (emphasis added).

49 NCTA Opposition at 10-11.

transfer of control has occurred.[50] The Act also sets terms for station licenses.[51] By contrast, most equipment authorizations do not have a specified term (unless the authorization was granted pursuant to a transition provision), and thus, there is no requirement to seek renewal of an equipment authorization. In short, NCTA's tortured attempt to equate an equipment authorization with a "station license" cannot be squared with the Act or the Commission's rules.

As to whether Part 15 devices are "authorized by or under this chapter" for purposes of Section 333, commenters do not dispute that the Act nowhere mentioned unlicensed services when Section 333 was enacted in 1990, nor do they deny that Congress did not amend the Act to expressly authorize "unlicensed" services generally until 1996. Instead, some commenters contend that this chronologic history is irrelevant to interpreting Section 333. They are wrong.

NCTA's view that the "chronologic order in which these provisions appeared in the Communications Act is immaterial to the interpretation of the statute's plain language as it exists today" is not shared by the Supreme Court.[52] Indeed, the Court frequently considers the plain meaning of the language at the time of enactment, as well as the chronologic order in which provisions are enacted, as relevant to statutory construction.[53]

---

50 47 C.F.R. § 2.929.

51 47 U.S.C. § 307(c).

52 NCTA Opposition at 5-6.

53 *See, e.g., Sandifer v. U.S. Steel Corp.*, 134 S. Ct. 870, 876-879 (2014) (interpreting the statutory term "changing clothes" to reflect Congress's presumed understanding of the term at the time of enactment as well as to reflect "the historical context surrounding § 203(o)'s passage"); *United States v. Fausto*, 484 U.S. 439, 453 (1988) ("it can be strongly presumed that Congress will specifically address language on the statute books that it wishes to change"); *BP Am. Prod. Co. v. Burton,* 549 U.S. 84, 99 (2006).

Petitioners agree that any interpretation of Section 333 must give meaning to its "plain language" and that the statute must be read as a whole.[54] Consistent with these canons of statutory construction, the language "licensed or authorized by or under this chapter" is properly understood to reflect Congress's intent to protect from interference: (i) stations that operate pursuant to a grant of an individual license under Section 307(a) ("licensed … by or under this chapter"); as well as (ii) stations that are not individually licensed but operate pursuant to a license granted by rule under Section 307(e) ("authorized by or under this chapter").

In addition to being harmonious with the plain language of Section 333, this interpretation is consistent with the statute's legislative history. As noted in the Petition, the legislative history confirms that Section 333 was intended to address the Commission's concern about interference to certain types of radio communications services – all of which operate pursuant to either an individual license or a license granted by rule.[55]

Some commenters contend that the "authorized by or under this chapter" should be read expansively to include Part 15 devices because they are "authorized" by the Commission pursuant to its general powers under the Act and because Congress was aware of the Commission's Part 15 rules when it enacted Section 333.[56] While this reading of Section 333 may be superficially appealing, it is fundamentally flawed in three respects.

First, there is an obvious distinction between a station that is expressly "authorized" pursuant to a regime enacted by Congress and a Part 15 device that may be "authorized" by a

---

54 *See, e.g.,* Google Opposition at 2; WISPA Opposition at 5-6; NCTA Opposition at 6.

55 S. Rep. 101-215 at 7 (Nov. 19, 1989); H.R. Rep. 101-316, at 8 (Oct. 27, 1989) (noting that Section 333 was enacted to address "instances of deliberate and malicious interference" to the following: (i) "amateur, maritime, and citizens band radio" services; (ii) "public safety radio services"; and (iii) "private land mobile, and cable television" services).

56 *See, e.g.*, WISPA Opposition at 7-8; Google Opposition at 2-3; NCTA Opposition at 7-8.

regime created by the Commission. Because unlicensed services were not expressly "authorized" by Congress under the Act when Section 333 was enacted in 1990, the plain language of the statute does not cover unlicensed services.[57]

Second, had Congress intended Section 333 to be as sweeping in scope as some commenters contend, there would have been no need for Congress to use the "licensed or authorized" language at all. Instead, Congress could have simply prohibited interference to any "radio communication," which plainly would have protected Part 15 devices from interference. Indeed, this was the approach embodied in S. 2975, which was introduced in 1984 with the following wording for Section 333: "No person shall willfully or maliciously interfere with or cause interference to any radio communication."[58] However, when Section 333 was reintroduced in 1990 as part of an FCC Authorization Bill, the language was narrowed to only prohibit interference "to any radio communications of any station licensed or authorized by or under this Act or operated by the United States Government."[59] Because Congress declined to use expansive language in enacting a prohibition against interference, Congress could not have

---

[57] NCTA argues that construing Section 333 to encompass Part 15 devices "captures the intentions of all the drafters of a statute, its original drafters as well as the drafters of subsequent amendments." NCTA Opposition at 7. But the Supreme Court has indicated that later enacted amendments are an unreliable guide for ascertaining the meaning of earlier enacted provisions: The Court has frequently observed "[T]he views of a subsequent Congress form a hazardous basis for inferring the intent of an earlier one." *Mackey v. Lanier Collection Agency & Serv., Inc.*, 486 U.S. 825, 839-40 (1988) (quoting *United States v. Price*, 361 U.S. 304, 313 (1960) and collecting cases). And the Court has rejected arguments premised on the idea that Congress seemed to manifest agreement with the parties' respective interpretations in later legislation. *See MCI Telecommunications Corp. v. Am. Tel. & Tel. Co.*, 512 U.S. 218, 233 (1994); *Mackey v. Lanier Collection Agency & Serv., Inc.*, 486 U.S. 825, 839 (1988) ("[T]he opinion of this later Congress as to the meaning of a law enacted 10 years earlier does not control the issue").

[58] *See* S.2975, 98th Congress (Sept. 10, 1984).

[59] *See, e.g.,* Cong. Rec. S10117-21, Senate debate on HR 3265 (July 19, 1990).

intended this prohibition to be interpreted expansively, notwithstanding claims by some commenters otherwise.

Third, to read "authorized by or under this chapter" to encompass Part 15 devices would create an obvious and irreconcilable conflict with the Commission's Part 15 rules. As explained in the Petition, willful interference to a Part 15 device does not violate the Commission's Part 15 rules because those rules prohibit "harmful interference," which in relevant part requires interruption to a "radiocommunications service"– a defined term that does not encompass Wi-Fi or any other Part 15 device.[60] No commenter disputes Petitioners' reading of the Commission's Part 15 rules. Yet no commenter offers a plausible explanation for how Section 333 lawfully could be interpreted to prohibit interference to a Part 15 device when such interference is not prohibited by the Part 15 rules under which the device is authorized to operate.[61] Because Congress was undoubtedly aware of the Commission's Part 15 regime when it enacted Section

---

[60] *See* 47 C.F.R. § 15.3(m); 47 C.F.R. § 2.1; *see also Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems*, 17 FCC Rcd 13522, ¶ 7, n.7 (2002) (because "Part 15 devices are not part of a 'service,' ... interference caused to a Part 15 device by another Part 15 device does not constitute harmful interference"). That the definition of "harmful interference" excludes interference to a Part 15 device is fatal to the assertion that interference to a Part 15 device violates 47 C.F.R. § 15.5(c). OTI/PK Opposition at 10. Notably, Section 15.5(b) of the FCC rules prohibits a Part 15 device from causing "harmful interference," but does not use the term "harmful interference" in describing the interference that a Part 15 device must accept. Rather, the rule conditions operation of the Part 15 device by stating "that interference must be accepted that may be caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator." *See also* 47 C.F.R. § 15.19 (setting forth the legend that must appear on the label of a Part 15 device).

[61] NCTA's attempt to reconcile its interpretation of Section 333 with the Commission's Part 15 regime is predicated on an erroneous understanding of the term "willful" as used in the Act, which is discussed below. *See* NCTA Opposition at 16-17 (reading Part 15's prohibition on "harmful interference" to apply regardless of the intent of the device operator, while interpreting Section 333 to only prohibit "willfully transmitting a signal with the purpose of preventing others from transmitting on that channel").

333, there is no reason to believe that Congress intended the statute to protect Part 15 devices from interference when the Commission's Part 15 rules expressly permit such interference.[62]

Indeed, interpreting Section 333 to protect Part 15 devices from interference is even more implausible given that the statute was enacted to address perceived gaps in the Commission's enforcement authority.[63] No such gaps exist under the Part 15 regime. The Commission established the "commons model" that is the hallmark of Part 15 – a model that the Commission could change on its own, if it were so inclined, without the need for Congressional action.[64]

That Section 333 does not prohibit interference to Part 15 devices does not mean that the Commission is powerless to adopt rules to address such interference, as OTI and PK erroneously contend.[65] On the contrary, Section 302 plainly authorizes the Commission to adopt "reasonable regulations" that govern "the interference potential of devices ...."[66] Indeed, adopting rules governing interference to Part 15 devices that appropriately balance the competing interests involved is a far superior regulatory vehicle, given that Section 333 purports to serve as an

---

62 *See* Cisco Comments at 18 ("It simply cannot be that a Part 15 device is both unprotected against interference under Section 15.5(b) but protected against interference under Section 333"); Smart City Comments at 11.

63 H.R. Rep. 101-316, at 8 (Oct. 27, 1989) ("Lacking any general statutory prohibition in the Communications Act of 1934 against willful or malicious interference, the Commission is forced to rely upon the more limited licensed operator provision of the Act concerning interference").

64 That legislation was not necessary to address interference to Part 15 devices also explains why Part 15 devices were omitted from the legislative history of Section 333 identifying the services the statute was intended to protect, and Google's attempt to explain away this omission is unconvincing. Google Opposition at 3.

65 OTI/PK Comments at 1-2. Nor does it mean that the Commission lacked the authority to adopt the Part 15 regime. It simply means that the "authorized by or under this chapter" language in Section 333 has a narrower scope than some commenters contend.

66 47 U.S.C. § 302a(a)(1).

absolute bar, prohibiting even "interference" undertaken for good cause, such as a documented security threat.

The Commission has never previously considered any of the threshold and definitional issues that would have to be resolved in order to interpret Section 333 to prohibit "interference" to Part 15 devices. The Petition provides the Commission with the opportunity to do so. For the agency to stick its head into the regulatory sand, as some commenters urge, is not a viable alternative. Ignoring the issues raised in the Petition will not make these issues go away, nor would doing so provide either Wi-Fi operators or consumers with the regulatory certainty they should reasonably expect from the Commission.

D. Interpreting Section 333 To Apply To Part 15 Devices Would Lead To Illogical Results.

Certain commenters take issue with Petitioners' argument that interpreting Section 333 to prohibit interference to Part 15 devices would lead to unintended and illogical consequences. For example, WISPA asserts that Petitioners "distort reality" by asserting that a homeowner using her cordless telephone that interferes with a neighbor's phone would face legal exposure under an expansive construction of Section 333; according to WISPA, because "the user's intent is only to complete the call, not to interfere with the use of another nearby device," that the user "inadvertently interferes" with another Part 15 device would not violate Section 333.[67] Other commenters make similar assertions.[68]

However, these assertions cannot be reconciled with the plain language of the Act or Commission precedent. The Act provides that "[t]he term 'willful', when used with reference to

---

[67] WISPA Comments at 10.

[68] *See, e.g.,* NCTA Opposition at 13-14; OTI/PK Opposition at 15 ("absent any specific knowledge or intent to interfere, all parties are on an equal footing and blameless vis-á-vis Section 333 and the Part 15 rules).

the commission or omission of any act, means the conscious and deliberate commission or omission of such act, *irrespective of any intent* to violate any provision of this chapter or any rule or regulation of the Commission authorized by this chapter or by a treaty ratified by the United States."[69] According to longstanding FCC precedent, a finding of willfulness "requires only that the Commission establish that the licensee knew that he was doing the acts in question – in short, that the acts were not accidental."[70] As the Commission has explained:

> Willfulness exists if there is a voluntary act or omission in that a person knew that he was doing the act in question, such as using a radio transmitter, as opposed to being accidental (for example, brushing against a power switch turning on a radio transmitter). Furthermore, to establish a willful violation, it is not necessary to show that a person knew he was acting wrongfully.[71]

Thus, WISPA's arguments notwithstanding, a homeowner acts "willfully" within the meaning of Section 333 when he or she knowingly operates a cordless telephone and thus stands in legal jeopardy under an expansive interpretation of the statute if such operation causes "interference" to another Part 15 device.[72]

In addition to being inconsistent with Commission precedent, NCTA's argument that "a person must intend to interfere with the signal of others" in order to violate Section 333 is not

---

69 47 U.S.C. § 312(f)(1) (emphasis added).

70 *Hubbard Broadcasting*, 1 RR2d 499, ¶ 6 (1963).

71 *Robert J. Hartman Cessapolis, MI*, 9 FCC Rcd 2057, ¶ 8 (1994); *see also Fayetteville Cellular Telephone Company L.P.*, 12 FCC Rcd 1385 (1997) ("A violation of FCC rules which results from inadvertent mistake is still considered a willful violation").

72 NCTA's claim that the Commission has never brought an enforcement action against "housewives and other innocent users of Part 15 devices" – while true – is irrelevant. NCTA Opposition at 13. Indeed, until the investigation of and resulting consent decree with Marriott, there is no indication that the Commission has ever sought to take enforcement action against any Part 15 device operator for interfering with another Part 15 device.

supported by judicial decisions interpreting the term "willful" under the Commissions Act.[73] These decisions confirm that willfulness does not require "bad faith" or an "evil purpose" as NCTA incorrectly asserts.[74]

E. Granting The Petition Would Not Harm Consumers Or Otherwise Adversely Affect The Commission's Part 15 Regime.

Several commenters offer dire predictions about various evils that supposedly will follow from any decision by the Commission to grant a declaratory ruling or initiate a rulemaking as requested in the Petition. None of these purported harms is persuasive or otherwise constitutes grounds to deny the Petition.

For example, OTI/PK's claim that granting the Petition would "create a new 'property right' in the spectrum based on land ownership" is meritless.[75] By addressing the issues in the Petition, the Commission can balance the interests of consumers and property owners with

---

[73] NCTA Opposition at 14. The three cases upon NCTA relies in defining the term "willful" are distinguishable. Two of the cases cited by NCTA do not even involve the Communications Act. *See Spies v. United States,* 317 U.S. 492 (1943) (income tax evasion in violation of Section 145(b) of the Internal Revenue Code); *United States v. Project on Gov't Oversight*, 616 F.3d 544 (D.C. Cir. 2010) (alleged violations of 18 U.S.C. § 209(a)). The third case – *Didricksen v. FCC*, 254 F.2d 354 (D.C. Cir. 1958) – simply stands for the unremarkable proposition that intent to violate the law is not required in order for an act to be "willful."

[74] For example, in *United States v. Baxter*, 841 F. Supp. 2d 378 (D. Me. 2012), the court upheld an enforcement action under Section 503(b)(1)(B) for violation of 47 C.F.R. § 97.101(d) which prohibits "willful[] or malicious[] interfere[nce]." According to the court, "Mr. Baxter insists that he did not set about to break the law. It makes no difference. What he did set about to do, deliberately, was to transmit at the dates and times the Government has alleged. This is enough." *Id.* at 395; *see also Primetime 24 Joint Venture v. Telecable Nacional*, No. CIV. A. 90-1941, 1990 WL 598572, at *2 (D.N.J. Oct. 10, 1990) ("The Federal Communications Commission interprets the term, 'willfully,' … as not requiring that the defendant know that he was acting wrongfully. It is enough that the defendant knew that 'he was doing the acts in question—in short, that the acts were not accidental'") (citation omitted)). The courts have applied this same approach to various uses of "willful" throughout the Act. *See, e.g., Maryland v. Universal Elections, Inc.*, 862 F. Supp. 2d 457, 463 n.7 (D. Md. 2012), *aff'd*, 729 F.3d 370 (4th Cir. 2013) (using Section 312(f)(1) to define "willful" violations of the TCPA).

[75] OTI/PK Comments at 13.

respect to the use of Wi-Fi services on private property. Petitioners believe that an appropriate balance can be struck that adequately protects these competing interests. By contrast, if the Commission decides to ignore the issues raised in the Petition as urged by some commenters, premise owners operating a Wi-Fi network may decide to prohibit or restrict the use of Wi-Fi devices on their property – a right commenters acknowledge property owners plainly have.[76] While lawful, such a prohibition or restriction on Wi-Fi usage could lead to some of the public harms about which commenters are supposedly concerned, not the least of which could be the effective creation of a land ownership-based property right in unlicensed spectrum to which OTI/PK objects.

Claims that permitting Wi-Fi operators to manage their networks to ensure a secure and reliable Wi-Fi service would threaten the public safety ring hollow.[77] Deauthentication of an unauthorized access point that poses a threat to the security or reliability of a Wi-Fi operator's network would not prevent a consumer from using her or her cellular connection to make a 911 call. Indeed, hotels are expending significant resources to improve cellular reception within their properties.[78] Even for those who may rely on VoIP technologies to make calls, a consumer is able to use other Wi-Fi access points to communicate when an unauthorized access point is subject to deauthentication; indeed, in certain circumstances, the effect of deauthentication can be avoided entirely "by moving the access point, or, in the case of wireless devices, simply by

---

76 *See, e.g.,* Google Comments at 10; Smart City Comments at 13, n.35.

77 Google Comments at 9 (claiming that allowing interference to Wi-Fi devices "could endanger guests on those properties" who "increasingly rely on Wi-Fi and VoIP technologies to make calls …"); WISPA Comments at 12.

78 *See* Hilton Comments at 5, n.3.

taking a few steps in one direction or another."[79] Thus, the impact of deauthentication on the ability of consumers to communicate is not nearly as draconian as some commenters suggest.

Furthermore, if a Wi-Fi operator has no ability to use deauthentication technology to ensure a secure and reliable Wi-Fi service, the airspace in high-density environments may become unusable by anyone. In this circumstance, "a 'tragedy of the commons' ensues such that the common resource of Part 15 spectrum becomes useless to all."[80] Such an outcome inevitably would have public safety implications that commenters opposing the Petition ignore.

As to arguments that any "interference" to unauthorized access points on a Wi-Fi operator's premises could disrupt other lawful Wi-Fi networks and devices outside of the operator's property, the answer is two-fold.[81] First, the deauthentication features of the network management equipment at issue in this proceeding are considerably more precise than some commenters suggest. For example, according to Smart City, it has developed a custom rule in the wireless protection policies built into its wireless controllers that only targets specific access points and devices located in high density areas, while having no impact on access points or devices in public or quasi-public areas.[82]

Second, to the extent a Wi-Fi operator takes action that adversely impacts users who are not physically located on its property, any network management rules or policies adopted by the Commission could make clear that the operator does so at its own peril. The remote possibility that deauthentication technology may adversely impact a nearby user or innocent bystander should not serve as a pretext to prohibit such use under any circumstances.

---

79 Smart City Comments at 14.

80 Hilton Comments at 4; *see also* Smart City Comments at 2.

81 OTI/PK Opposition at 17; WISPA Opposition at 11.

82 Smart City Comments at 12-13.

F. Commenters Opposing The Petition Misconstrue The Significance of the Commission's Equipment Authorization and OTARD Rules.

Commenters opposing the Petition largely ignore the inherent problem in finding that the deauthentication capability of Wi-Fi network management equipment violates Section 333 when such equipment has been authorized by the agency. While NCTA is correct that equipment authorization is not a "guarantee that the device will cause no harmful interference,"[83] the equipment authorization program "is one of the principal ways the Commission ensures that RF devices used in the United States operate effectively without causing harmful interference and otherwise comply with the Commission's rules."[84] The equipment authorization rules are "intended to prevent devices that could cause harmful interference to radio communications from reaching the marketplace or being operated."[85]

While even authorized equipment can be used improperly, under the view espoused by various commenters, network management equipment containing a deauthentication capability is the equivalent of a "jammer" and thus any use of this capability constitutes "interference" prohibited by Section 333.[86] Under this view, it would be irrelevant how the network management equipment actually "is being used."[87]

However, because network management equipment that includes the deauthentication capability is authorized by the Commission, such equipment does not constitute a "jammer" by definition, despite some commenters' repeated use of this pejorative term. Indeed, by

---

83 NCTA Opposition at 21.

84 *Amendment of Parts 0, 1, 2, and 15 of the Commission's Rules Regarding Authorization of Radiofrequency Equipment*, Report and Order, FCC 14-208, ¶ 3 (rel. Dec. 30, 2014).

85 *Amendment of Parts 0, 1, 2, and 15 of the Commission's Rules Regarding Authorization of Radiofrequency Equipment*, Notice of Proposed Rulemaking, 28 FCC Rcd 1606, ¶ 3 (2013).

86 CTIA Comments at 2-3; Microsoft Comments at 6-7; OTI/PK Opposition at 10.

87 Microsoft Comments at 6

authorizing the network management equipment at issue, the Commission necessarily has determined that such equipment complies with its Part 15 rules and that such equipment can be operated without causing "harmful interference" prohibited by Part 15. Under the circumstances, it would be beyond strange for the Commission to find that the operation of the equipment it has expressly authorized nonetheless causes "interference" prohibited by Section 333.

OTI/PK's solution to this problem is for the "Commission to immediately stop certifying" Wi-Fi network management equipment that "can easily be configured to jam [sic] third-party Wi-Fi transmissions ...."[88] But this "solution" would have no impact on the network management equipment already authorized by the Commission that is currently in the market or provide any comfort to the multitude of users that purchased such equipment to manage their Wi-Fi networks without notice that such equipment may violate Section 333. Furthermore, because deauthentication is part of the IEEE 802.11standard, OTI/PK does not explain how the Commission could approve any 802.11-compliant equipment if deauthentication technology is inherently violative of Section 333, as OTI/PK and several other commenters maintain.

As to the Commission's OTARD rules, there is no merit to NCTA's claim that Petitioners "read OTARD to mean that any property owner can use its antennas to block the reception of any signal on their property."[89] That is not how Petitioners read the Commission's OTARD rules and that is not what the Petition says. Rather, the Petition (p. 19) merely states that "[c]onstruing Section 333 to prohibit interference to Part 15 devices operated by guests of a hotel or similar venue would give such guests superior rights as compared to owners or lessors of property in their use of Part 15 devices."

---

88 OTI/PK Opposition at 14.

89 NCTA Opposition at 18.

The Commission's OTARD rules provide in relevant part: "Any restriction ... on property within the exclusive use or control of the antenna user where the user has a direct or indirect ownership interest or leasehold interest in the property that impairs the installation, maintenance, or use of [a covered device] ... is prohibited ...."[90] Consistent with the Commission's interpretation, OTARD prohibits any "restriction" on the "use" of a Wi-Fi device, provided that the device is "located on the property within the exclusive use and control of the antenna user where the user has a direct or indirect ownership or leasehold in the property."[91] Under the interpretation espoused by several commenters, by contrast, Section 333 prohibits the "restriction" on the "use" of a Wi-Fi (by means of "willful interference") of a Wi-Fi device used by an invitee or licensee who enjoys no rights under the Commission's OTARD rules.

To be sure, Section 333 and OTARD serve different purposes. But Petitioners point is merely that Section 333 cannot be read in isolation, and any proper interpretation of the statute as applied to Part 15 devices must be consistent with other provisions of the Act, including OTARD – a seemingly unremarkable proposition with which some commenters nonetheless take issue.[92]

---

[90] 47 C.F.R. § 1.4000(a)(1)(A).

[91] *See Continental Airlines Petition for Declaratory Ruling Regarding the Over-The-Air Reception Devices (OTARD) Rules*, Memorandum Opinion and Order, 21 FCC Rcd 13201, ¶ 12 (2006) (citing 47 C.F.R. § 1.4000(a)(1)). Although WISPA insists that OTARD provides no protection to the "transient presence of a device that may function as an access point," WISPA Opposition at 11, the language of the rule is considerably broader than WISPA suggests. *See also* OTI/PK Opposition at 15.

[92] NCTA's argument that "the OTARD regulations—a collection of administrative rules—cannot alter the meaning of Section 333, a statutory provision" is misguided. NCTA Opposition at 18. First, Petitioners do not contend that the Commission's OTARD rules should "alter" Section 333, but rather that these requirements should be interpreted in harmony. Second, the FCC's OTARD rules stem directly from Section 207 of the Telecommunications Act of 1996, which directed the Commission to "promulgate regulations to prohibit restrictions that impair a viewer's ability to receive video programming services through devices designed for over-the-air reception of television broadcast signals, multichannel multipoint distribution service, or direct broadcast satellite services." 47 U.S.C. § 303 Note.

III. CONCLUSION

The record confirms that considerable controversy and uncertainty exists regarding the application of Section 333 to Part 15 devices, which the Commission can resolve by granting the requested declaratory ruling or initiating a rulemaking proceeding. Regardless of the procedural vehicle, the Commission should provide much needed guidance to Wi-Fi operators about the reasonable measures they can employ in providing a secure and reliable Wi-Fi service.

Respectfully submitted,

Banks Brown
McDermott Will & Emery LLP
340 Madison Avenue
New York, NY 10173-1922
212 547 5488

Counsel for the American Hotel & Lodging Association

Bennett L. Ross
David E. Hilliard
Henry Gola
Wiley Rein LLP
1750 K Street, NW
Washington, DC 20006
(202) 719-7000

Counsel for Marriott International, Inc. and Ryman Hospitality Properties

January 5, 2015

CERTIFICATE OF SERVICE

I do hereby certify that, on this 5th day of January 2015, I caused copies of the foregoing "Reply Comments in Support of Petition for Declaratory Ruling or, in the Alternative, for Rulemaking" to be delivered to the following via First Class U.S. mail:

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

Brian M. Josef
Scott K. Bergmann
Michael F. Altschul
CTIA – The Wireless Association®
1400 16th Street, N.W., Suite 600
Washington, D.C. 20036

Harold Feld
Public Knowledge
1818 N St NW
Washington, DC 20036

Michael Calabrese
Patrick Lucey
Wireless Future Project / Open Technology Institute
1899 L St NW – 4th Floor
Washington, DC 20036

Paula Boyd
Microsoft Corporation
901 K Street, NW, 11th Floor
Washington, D.C. 20037

Michael Daum
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Austin C. Schlick
Stephanie Selmer
Google Inc.
25 Massachusetts Avenue NW, Ninth Floor
Washington, DC 20005

Rick Chessen
Neal M. Goldberg
Jennifer K. McKee
National Cable & Telecommunications Association
25 Massachusetts Avenue, NW, Suite 100
Washington, DC 20001

Charles Corbin
Ama Romaine
Hilton Worldwide Holdings Inc.
7930 Jones Branch Drive, 6th Floor
McLean, VA 22102
Counsel to Hilton Worldwide Holdings Inc.

Mark E. Crosby
Enterprise Wireless Alliance
2121 Cooperative Way, Suite 225
Herndon, VA 20171

Elizabeth R. Sachs
Lukas, Nace, Gutierrez & Sachs, LLP
8300 Greensboro Drive, Ste. 1200
McLean, VA 22102
Counsel to Enterprise Wireless Alliance

Mark Haley
Smart City Networks, LP
5795 W. Badura Ave., Suite 110
Las Vegas, NV 89118

Jonathan Banks
Robert Mayer
United States Telecom Association
607 14th Street, NW, Suite 400
Washington, D.C. 20005

Colleen Boothby
Levine, Blaszak, Block & Boothby, LLP
2001 L Street, NW, Ninth Floor
Washington, D.C. 20036
Counsel for Ad Hoc Telecommunications Users Committee

Marta Beckwith
Aruba Networks
1344 Crossman Ave.
Sunnyvale, CA 94089

Patrick Rousseau
203 Harrison Place
Brooklyn, NY 11237

Mark Saurman
755 Sparrow Way
Wadsworth, OH 44281-7718

Paul Rauner
SirenGPS, Inc.
9272 Olive Street
St Louis, MO 63132

Glen E. Ashman
2791 Main Street
East Point, GA 30344

Peter Tannenwald
Fletcher, Heald & Hildreth, PLC
1300 N. 17th St., 11th Floor
Arlington, VA 22209
Counsel for Brown University

Mary L. Brown
Cisco Systems, Inc.
601 Pennsylvania Avenue, NW
9th Floor North
Washington, DC 20004

Scott Maples
Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089

Jason Embee
Post Office Box 1
Berwick, PA 18603-0001

Arnold G. Reinhold
14 Fresh Pond Place
Cambridge, MA 02138

Nathaniel Cade, Jr.
P.O. Box 170887
Milwaukee, WI 53217

David T. Witkowski
1525 Altamont Ave.
San Jose, CA, 95125