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 CISCO SYSTEMS, INC.

Mary L. Brown
Director, Government Affairs
Cisco Systems, Inc.
601 Pennsylvania Avenue, NW
9th Floor North
Washington, DC 20004
(202) 354-2923

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
CISCO SYSTEMS, INC.

On August 25, 2014, the American Hotel & Lodging Association, Marriott International, Inc., and Ryman Hospitality Properties petitioned the Commission for a declaratory ruling interpreting Section 333 of the Communications Act of 1934, as amended,[1] as permitting the operator of a Wi-Fi network operator to manage the use of Wi-Fi on its premises, even if doing so "may result in 'interference with or cause interference' to a Part 15 device being used by a guest on the operator's property."[2] In the alternative, the Hotel Petition urges the Commission to commence a rulemaking proceeding to amend Part 15 to provide clarity regarding the ability of property owners to manage unlicensed operations on their property.[3] Cisco Systems, Inc. ("Cisco") submits these comments in response to the Commission's solicitation of input on the Hotel Petition.[4]

---

[1] 47 U.S.C. § 333.

[2] 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, at 1 (filed April 25, 2014)("Hotel Petition"). *See also id.* at 13-19.

[3] *See id.* at 19-21.

[4] *See* "Consumer & Governmental Affairs Bureau Reference Information Center Petition for Rulemaking Filed," *Public Notice*, Report No. 3012 (rel. Nov. 19, 2014).

I. INTRODUCTION AND EXECUTIVE SUMMARY

Since its inception in 1984, Cisco has become the world's largest provider of networking technology, equipment, solutions and services used in the deployment and management of next-generation broadband networks. Among other things, Cisco has been a global leader in the manufacture of products based on the IEEE 802.11 family of standards for unlicensed wireless local area network devices, developing a range of wireless access points, controllers, antennas and integrated management tools that meet the unique needs of the enterprise and service provider segments of the marketplace. Cisco is an active participant in the IEEE 802.11 standard setting process and the Wi-Fi Alliance interoperability forum.[5] As such, Cisco is vitally interested in the issues raised by the Hotel Petition.

Unlicensed spectrum generally should be open and available to all who wish to make use of it, but access to unlicensed spectrum resources can and should be balanced against the need to protect networks, data and devices from security threats and potentially other limited network management concerns. For example, in public places or places where the public is routinely invited, users have every reason to expect that they can make use of personal hot spot technology, unless the user's device is presenting a security threat of some type to the co-located enterprise or service provider Wi-Fi network. That balance shifts in enterprise locations,[6] where

[5] IEEE 802.11 is the industry standards forum where much of the wireless local area network (WLAN) technology for "Wi-Fi" radio systems is standardized. The Wi-Fi Alliance is the industry's interoperability forum that exists to ensure that different manufacturers' implementations of Wi-Fi can interoperate. Some of the Alliance's work also further enhances the standards work from IEEE 802.11. The term "Wi-Fi" can commonly be used to refer to a Wi-Fi enabled radio device or a network that supports Wi-Fi radios, and technologists would also interpret "Wi-Fi" to imply the use of 802.11 standards-based technologies. We use both terms in this comment.

[6] For purposes of these comments, the term "enterprise" will be used to reference governmental agencies, educational institutions, hospitals, and private entities that deploy wired or wireless networks to carry their own internal data and/or that or their guests.

many entities use their Wi-Fi networks to convey company confidential information, trade secrets, and for the safety and security of the firm and its employees. In these situations, enterprises must be able to assert policies on the use of wireless technologies for employees and guests in order to safeguard the network, data and devices. This is not a problem limited to critical infrastructure firms or sensitive government installations, but can extend to any enterprise. Similarly, service provider Wi-Fi networks are used by members of the public with the expectation that their data and devices will be secure, and service providers must have the flexibility to use network management technology to meet that expectation.

In our comments, below, Cisco asserts the following:

First, Cisco supports the view expressed in the Hotel Petition that use of 802.11-based network management security technologies does not constitute interference under Section 333, and therefore does not constitute "jamming" of another device. The application of Section 333 to Wi-Fi security technologies is wrong on the law and wrong on the facts. Section 333 cannot be interpreted to protect unlicensed devices from interference because unlicensed devices are not "stations" for purposes of that Section and, under Section 15.5(b) of the Commission's Rules, unlicensed devices are not entitled to interference protection. Moreover, in any event, Section 333 applies only to electromagnetic interference, which is not present in the use of standards-based network management tools. The Commission should use the opportunity presented by the Hotel Petition to re-orient its views on these matters. Failure to do so essentially de-values the use of Wi-Fi in enterprise and service provider environments, because the technology at issue here is the same technology that protects Wi-Fi networks now in widespread throughout our economy.

Second, Cisco agrees that personal hot spot technology users should have an expectation that they can use their devices anywhere and anytime, absent a security threat, or potentially in a few other limited cases. If a device is in normal operation, not presenting a security threat, and the user is in a public space or a space where the public is routinely invited, then network administrators of the co-located enterprise or service provider network should not attempt to contain the device.

Third, Cisco strongly urges the Commission, either itself or through staff action, to issue a policy statement on the network management issues presented when security tools are in use. Carefully crafted, a policy statement would have a beneficial effect of ensuring that all network administrators are on notice of what they can and should do when managing networks, data and a devices that make use of unlicensed spectrum. This will bolster efforts by manufacturers in communicating with customers about the technology and its uses. At a minimum, such a policy statement should encourage Wi-Fi network operators to only utilize IEEE 802.11 management frames to disrupt the operation of unmanaged or unauthorized Wi-Fi devices on their premises when doing so addresses security or other legitimate concerns. Moreover, before additional enforcement actions are taken on similar facts to the Marriott case, the Commission would be well served to resolve this proceeding, issue a policy statement, and provide an opportunity for network administrators to come into compliance with it.

Fourth, Cisco opposes the suggestion that the Commission proceed to a rulemaking at this time. Make no mistake – Cisco recognizes that operators of Wi-Fi networks should not have *carte blanche* to disrupt the operation of Wi-Fi or other unlicensed devices without legitimate justification. At the same time, those that would abuse the power of Wi-Fi for illegitimate ends are clever and industry is constantly playing "catch up" as new techniques for abuse are

developed. As a result, it would be a mistake for the Commission to take a snapshot of the current situation and develop a comprehensive regulatory regime that could preclude industry from addressing new threats as they arise.

In the comments below, Cisco describes the security technology that safeguards networks, data and devices, permits a network administrator to order containment of a particular transmitter, and highlights some of the security considerations that network administrators face every day. Next, Cisco presents our view that use of such technology does not constitute "interference" under Section 333, and that in any event, Section 333 cannot protect unlicensed devices from interference as a matter of law. Finally, Cisco urges the Commission to adopt policy guidance for network administrators when using security technology, while opposing a rulemaking at this time.

In this comment, we will use the term "managed" devices to refer to Access Points ("APs") and Client Devices that a network administrator has installed or approved for use on its network. "Unmanaged" devices are those that the managed network can see, but are not part of the network, such as a personal hot spot or nearby Access Point or client device that are part of someone else's network. "Unauthorized" is used as a term to describe an Access Point that has been wired into an entity's Wi-Fi network, such as if an employee brought in an Access Point from home and added it to an enterprise network without the permission of the network administrator. Cisco urges the Commission to adopt a clear syntax (this, or a similar one) to ensure that any further Commission statements in this area are as clear as possible, as vendor

marketing material varies widely. The term "rogue" AP is often used, but lacks the precision that we suggest here.[7]

II. NETWORK SECURITY TOOLS ARE REQUIRED TO PROTECT WI-FI NETWORKS, DATA ACCESSIBLE ON OR THROUGH THOSE NETWORKS, AND DEVICES

Those in the private sector and government who operate networks face a wide range of challenges in maintaining security – operators must maintain security of their networks, security of information (both their own and that entrusted to them by third parties), security of the devices, and data of those invited onto their premises. The growth of wireless networking and the sheer number of new mobile computing devices available to users has challenged the traditional boundaries between trusted and untrusted networks. In addition, the rise of "Bring Your Own Device" to work has raised the stakes considerably for network managers that must allow wanted communications to and from approved devices, while disallowing communications with unwanted ones. The expanded availability of IEEE 802.11 Wi-Fi devices (and the concomitant growth in demand for mobile access to information) creates a unique dichotomy for network managers, demanding more open networks and freedom of access to information, while at the same time meeting security imperatives that often demand more restrictive access and more control.

[7] Wi-Fi networks can be as simple as a Wi-Fi AP that is wired to a broadband connection in a residential household, providing short-range wireless services to registered client devices in the home. Wi-Fi networks can also be quite complex, consisting of mesh node architectures, range extenders, bridges, relays, and/or wireless controllers (including security), in addition to managed APs and client devices. Deployments also exist that place much of the Wi-Fi network intelligence, including security, in the cloud. For present purposes, the comment here simplifies the architecture to APs, sometimes called "masters" in industry literature, and client devices that authenticate and associate to those APs. Security capability is provided to the APs and client devices from a wired network or via a cloud-based service delivered through the wired network.

Among the myriad security threats faced by those charged with network management are several that can particularly affect IEEE 802.11 Wi-Fi networks:

- Unauthorized APs can be added to an otherwise secure network, sometimes by well-meaning staff merely looking for Wi-Fi access and sometimes by persons seeking access to the network with malicious intent. In either case, these unauthorized APs circumvent security measures the network operator has applied to limit network access, and may result in managed client devices connecting to the unauthorized AP.

- Government agencies, educational institutions and enterprises often have specific policies limiting the nature of the information permitted to traverse their networks. These could fulfill legal requirements or simply corporate policy. By setting up an unauthorized AP, or operating an unmanaged one, the network, an employee, guest or intruder can circumvent these data security and other content policies.

- Another instance in which unmanaged APs can be problematic involves what the Hotel Petition calls a "honey pot" attack. In these attacks, the unmanaged AP uses an SSID that is designed to lure unsuspecting client devices into connecting to the honey pot by broadcasting a confusing SSID. This type of attack is generally done in public or quasi-public spaces where it is (a) easy to set up a hidden AP and (b) guests/customers don't know the exact name or SSID of the legitimate network. For example, an unmanaged AP could be activated in the Commission meeting room with the SSID "FCC Guest Network", hoping to attract guests looking to access the FCC's own guest network, which has the SSID of "FCC HotSpot Network". Once connected, the victim client device of the "honey pot" attack is vulnerable to man-in-the-middle, Address Resolution protocol poisoning, DHCP/DNS hijacking and injection of network worms and viruses, among other threats.[8]

- In addition, unmanaged Ad Hoc devices (personal hot spots), if associated with a co-located Wi-Fi network, can rebroadcast that network's SSID, essentially acting as a bridge. This creates a gateway to the co-located Wi-Fi network that a hacker can exploit.

- Unauthorized or unmanaged APs can be used to launch denial of service attacks that can disrupt or disable a Wi-Fi network. These are attempts to prevent client devices from associating with a legitimate AP by transmitting an excessive number of messages to clients.

- The opposite of denial of service attacks are packet floods, where the client devices or APs send an excessive number of packets to a managed AP disrupting the normal operations of that AP.

[8] *See* Hotel Petition at 7.

Fortunately, the Wi-Fi industry has provided network administrators with a range of tools to battle back against these threats. In addition to the technologies from Aruba Networks, AirTight Networks, Cisco and Fluke Networks cited in the Hotel Petition,[9] many others provide network managers with software and hardware tools for mitigating these security risks and otherwise managing access to the network. Although these tools vary from vendor to vendor, they are generally designed to enhance the ability of enterprises to establish and enforce policies that protect networks, data and devices. Given the importance of protecting against these threats, it is not surprising that in 2012, the Information Technology Laboratory at the National Institute of Standards and Technology issued a report, "Guidelines for Securing Wireless Local Area Networks (WLANs)," that strongly recommends the use of these sorts of network management tools to secure networks.[10]

One of the most common techniques used to manage Wi-Fi use on a network operator's premises involves the transmission of IEEE 802.11 deauthentication frames that "contain" unauthorized or unmanaged APs or client devices. Indeed, it is the use of that technique that led to the October 3, 2013 Consent Decree between the Enforcement Bureau and Marriott International, Inc., and Marriott Hotel Services, Inc. (collectively, "Marriott").[11] Because containment through deauthentication is one of the primary tools used by many network management systems to mitigate security threats and otherwise manage access, it is important to understand the role that deauthentication plays under the IEEE 802.11 standard.

---

[9] *See id.* at 8-9.

[10] Information Technology Laboratory at the National Institute of Standards and Technology, "Guidelines for Securing Wireless Local Area Networks (WLANs)," Special Publication 800-153, at *available at* *http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf*

[11] *See* Marriott Int'l, Inc., *et al,* File No. EB-IHD-13-00011303 (rel. Oct. 3, 2014)(the "Marriott Consent Decree").

The deauthentication frame is just one of several types of management frames defined under Section 10.3 of the IEEE 802.11 standard – others include the authentication frame, the association request frame, the association response frame, and the disassociation frame. Before a client device can access the resources of a Wi-Fi network, it engages in a process of authentication and association with the relevant AP by exchanging a series of management frames that provide a technical "hand shake" between the two devices and allow the AP to reject a connection based on policies set by the network operator. Even once authentication and association under 802.11 have occurred, the network operator may impose additional security measures that must be met before a client device can access network resources (the most common being a splash page requiring the entry of a password or other identifying information).

APs are bridges for traffic between client devices and other resources on the network (data storage devices, Internet access, etc.). Before a client device can send traffic through an AP, it must be in the appropriate connection state. The four connection states under Section 10.3.1 of the IEEE 802.11 standard are:

- State 1 -- Not authenticated or associated.
- State 2 -- Authenticated but not yet associated.
- State 3 -- Authenticated and associated (pending completion of any implemented Robust Security Network authentication).
- State 4 – Authenticated and associated.

Generally, a client must be in State 4 (both authenticated and associated) before bridging will occur and the client can fully access network resources. While limited management communications occur during States 1 and 2, the client cannot access the network resources while the connection is in those States.

When a client device enters into range of an AP, the two devices start out in State 1 (not authenticated and associated). A client device, when active, sends probe requests to discover IEEE 802.11 networks within its proximity and to provide information regarding the client's technical compatibility. A client device may also learn about the IEEE 802.11 networks within its proximity from Beacons regularly transmitted by the APs. Every AP that receives the probe request then checks to see if the client is technically compatible with it. If so, the AP generally responds to the probe request by providing the client with essential technical information regarding the AP. The client then selects from among the identified APs and attempts authentication by sending an authentication frame to the AP or APs of its choice.[12]

If the AP is configured for the most common type of authentication, "open authentication", it will immediately respond to the client's authentication frame with a frame establishing authentication and moving the connection to State 2. If a different type of authentication is employed, the AP will engage in other checks to validate the client before completing authentication.[13]

Once authentication is completed and the connection moves to State 2, the client device then executes the association process, after which the devices are in State 3 (if RSNA security is required) or State 4 (if RSNA security is not required). Devices in State 3 transition to State 4 after the RSNA process completes. In State 4, full access to the network is possible. Deauthentication returns a device to State 1 and disassociation (or a failed RSNA certificate) returns it to State 2. Deauthentication packets are sent for many reasons – the client leaves the vicinity, the client goes to sleep, a security tool is invoked, or for other reasons.

[12] A client can be 802.11 authenticated to multiple APs, but can only be actively associated with one at a time.

[13] Note that 802.11 authentication is not the same as the RSNA authentication mechanisms, which occur after the mobile stations is authenticated and associated.

The management frame structure for forming a Wi-Fi network (or taking it apart), have been used as the basis for various vendor security and network offerings. To meet the security needs of enterprise and home users alike, the management capabilities of IEEE 802.11 have been transformed by vendors into security solutions, used to identify potential threats, to exclude those without the proper credentials, take action against specific security threats, and to generally manage access to Wi-Fi networks. While each provider has its own implementation, all take advantage of various IEEE 802.11 management frames.

As noted above, in ordinary operations of a Wi-Fi network, a deauthentication frame can be sent by either a client device or an AP and, upon receipt, is interpreted by the receiving device as a termination of its connection with the other device. A deauthentication frame is often sent in the ordinary course of setting up or taking apart a network.

These network management functions exist because Wi-Fi networks have no single network manager controlling access to spectrum resources. It is at the heart of the IEEE 802.11 standard that Wi-Fi access points and client devices are continually seeking each other out, seeking to form networks and negotiating the terms of connection. There are a wide variety of significant reasons why connections should not be allowed to form. For example:

- A governmental entity or corporation may not wish to have anyone visiting its premises to access its corporate network for security reasons.
- A home user wants to lock its network with a password to better secure personal data and other devices.
- An access point may want to turn away additional client devices because it does not have enough ports to support the volume of users.
- Someone may maliciously be trying to lure client devices with an unauthorized or unmanaged AP to obtain data from the corporation.
- K-12 schools (and libraries and others) are required to comply with the Children's Internet Protection Act. In order to do so, schools usually set up Internet filtering software to prevent minors from viewing adult content and other

unauthorized Internet sites at school (or the library). Savvy students can set up unauthorized or unmanaged APs and get around these content filters.

- Unmanaged APs can use spectrum resources in a way that slows the throughput of an entity's own wireless network. In certain circumstances, such as hospitals or portions of hospitals, this can impact important/critical or time sensitive functions that depend upon the managed Wi-Fi network.

From the above description, the Commission can and should conclude that the technology, cited in the Marriott enforcement case, has many legitimate and beneficial uses, and indeed is built from the same technology used by Wi-Fi systems to form or take apart networks.

In enterprise or service provider Wi-Fi security offerings generally, the security tools give the network administrator a view into both managed and authorized access points that are operational, as well as unmanaged or unauthorized access points and client devices. If unmanaged or unauthorized access points are present, the network administrator needs to determine, for example, if a security risk is present. The security tools typically provide the network administrator some information about the behavior of the unmanaged or unauthorized transmitter and its location. In some cases, it will be clear that a device is implicated in a direct security threat, such as it is broadcasting a confusing SSID and attracting managed client devices to associate with it. In other cases, such as in multi-tenant office buildings, the network administrator will see other legitimate SSIDs of nearby Wi-Fi networks. Or perhaps a network administrator sees an unmanaged AP operating in a location where no unmanaged wireless devices are permitted, such as in a highly restricted area. The network administrator then needs to make a judgment call about whether to invoke containment technology.[14] The technology

[14] For example, some security tools allow administrators to mark neighboring known non-interfering APs as friendly, or to make lists of APs to ignore. In either case, the marked or listed APs would not be subject to future containment activity.

does not make the determination independently.[15] Network administrators need to be mindful that, if not carefully administered, containment can become a blunt instrument that contravenes reasonable expectations regarding Wi-Fi availability.

Once a decision is made to use containment, the security tool causes the managed network to issue deauthentication and/or disassociation frames. The unauthorized or unmanaged AP would interpret these frames as the client requesting deauthentication or disassociation, while the client device interprets the frames as the unauthorized or unmanaged AP requesting deauthentication or disassociation. The result is that the network between the unauthorized or unmanaged AP and the client device is forced back to State 1 or 2. The user experience is simply that its connection to the Wi-Fi AP won't work.

III. THE COMMISSION SHOULD DECLARE THAT SECTION 333 IS NOT IMPLICATED WHEN A WI-FI NETWORK OPERATOR USES DEAUTHENTICATION OR OTHER PROVISIONS OF THE IEEE 802.11 STANDARD TO CONTAIN UNMANAGED OR UNAUTHORIZED TRANSMITTERS

A. THE TRANSMISSION OF DEAUTHENTICATION FRAMES DOES NOT RESULT IN INTERFERENCE

Section 333 states 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 Act or operated by the United States Government."[16] It is unfortunate that the Hotel Petition uses the misnomer "interference" to describe how Wi-Fi network operators treat unauthorized or unmanaged Wi-Fi operations on their premises.[17] As described above, among the most common

[15] Some network management systems allow administrator to order the security tools to apply administrator-selected default configurations under which the network will contain unauthorized or unmanaged APs under certain circumstances without further manual intervention.

[16] 47 C.F.R. § 333.

[17] *See, e.g.* Hotel Petition at 1.

tools available for network administrators to use when deploying managed Wi-Fi networks in environments where unauthorized or unmanaged Wi-Fi transmissions could occur is the use of the IEEE 802.11 deauthentication frame – one of the network management techniques presented in the Hotel Petition and the one at issue in the Marriott Consent Decree.[18] An AP's transmission of a deauthentication frame to a client does not constitute interference for purposes of Section 333.

Interference is defined by the Commission as "[t]he effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy."[19] It occurs when a receiver is adversely impacted by the electromagnetic field existing in the radio frequency. "Jamming", which is the transmission of "powerful radio signals that overpower, jam, or interfere with authorized communications," is the intentional causation of interference through an increase in the unwanted signal being received by the victim receiver (as measured by signal-to-noise or carrier-to-interference signal levels).[20] The wanted signal is still present, but the electromagnetic signal from the jammer has raised the level of unwanted electromagnetic energy to the point that the receiver cannot properly receive it.

---

[18] Marriott Consent Decree at ¶ 5.

[19] 47 C.F.R. § 2.1.

[20] *See* C.T.S. Technology Co., Limited, *Notice of Apparent Liability for Forfeiture and Order*, 29 FCC Rcd 8107, 8107-08 (2014)("*C.T.S. NAL*"). *See also* "FCC Enforcement Advisory: Cell Jammers, GPS Jammers and Other Jamming Devices," *Public Notice*, DA 11-250 (Enf. Bur. 2011). Although the Marriott Consent Decree references that the initial informal complaint against Marriott alleged jamming, it does not suggest that the Enforcement Bureau believes that containment through the transmission of deauthentication frames constitutes jamming. Certainly, a Wi-Fi device can be jammed through the transmission of very high levels of unwanted energy that overpower the Wi-Fi radio, but that is not at issue here.

The facts that form the basis of the Declaratory Ruling request do not involve interference or the use of jammers – devices that "have no lawful consumer use in the United States."[21] An AP (a device that clearly has lawful use) that transmits an IEEE 802.11 deauthentication frame to contain an AP or other device is not a jammer and the signal it transmits does not cause electromagnetic interference. Other than the client device being deauthenticated, the signal has no impact on any other Wi-Fi or other unlicensed device. It is how the recipient translates the information in the frame that results in the termination in the connection, not the RF characteristics of the signal. There is no change in the signal-to-noise, carrier-to-interference ratio, or other measure of interference. All that is happening is a standards-based exchange of network management information using defined protocols. The Commission should not conflate network management practices with interference or jamming.

B. SECTION 333 DOES NOT PROTECT PART 15 DEVICES

Even if one assumes for purposes of discussion that the sending of an IEEE 802.11 deauthentication frame causes "interference" (which it does not), the sending of such frames cannot constitute a violation of Section 333 of the Act because Section 333 does not protect unlicensed devices operating under Part 15. Section 333 only protects "stations", and unlicensed devices operating pursuant to Part 15 are not "stations."

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 Act or operated by the United States Government." (emphasis added). To resolve the controversy caused by the Enforcement Bureau's stated belief that Section 333 protects

[21] *See C.T.S. NAL*, 29 FCC Rcd at 8107-08. *See also* "FCC Enforcement Advisory: Cell Jammers, GPS Jammers and Other Jamming Devices," *Public Notice*, DA 11-250 (Enf. Bur. 2011).

unlicensed Part 15 devices, the Commission can and should declare that because Part 15 unlicensed devices are not "stations" for purposes of the Act, one cannot violate Section 333 by interfering with or causing interference to a Part 15 device. While the text of Section 333 does not define what constitutes a "station," other provisions of the Act and the Commission's rules support the interpretation that Part 15 devices do not fall within the scope of "stations" entitled to protection.[22]

Aside from Section 333, Title III of the Act contains numerous provisions regarding "stations", including:

- Sections 307 and 308, which set out the requirements for "station" applications, licenses, modifications, and renewals.[23]
- Section 309, which establishes processes for Commission action on applications for a "station" license, modification, or renewal under Section 308.[24]
- Section 310, which includes certain ownership limitations on, and requirements for the assignment of license and transfer of control of, "station" licenses."[25]

The Commission has recognized that not all intentional radiators are "stations" and has never imposed the licensing requirements applicable to "stations" under these provisions of Title III on Part 15 devices.[26] To the contrary, the Commission has recognized that Congress intended for

[22] Section 3 (35) of the Act defines the terms "radio station" or "station" as "a station equipped to engage in radio communication or radio transmission of energy." 46 U.S.C. §147(35). Unfortunately, this circular definition (for equipment to constitute a station, it must be a station) is not itself particularly enlightening as to the scope of Section 333.

[23] 47 U.S.C. §§ 307, 308.

[24] 47 U.S.C. § 309.

[25] 47 U.S.C. § 310.

[26] We note that Section 307(e) of the Act allows for "radio stations" to operate without individual licenses in certain specified radio services (the citizens band radio service; the radio control service; the aviation radio service; and the maritime radio service), 47 U.S.C. § 307(e). However, Part 15 devices are not covered by this unique "license by rule" regulatory regime.

there to be a regulatory regime under which low-power devices can be operated without the individual licensing burdens of Sections 307 to 310 of the Act – a regime contained in Part 15.[27]

Were the Commission to find that a Part 15 device is protected from interference under Section 333, it must necessarily conclude that the device is a "station." But, if a Part 15 device is a "station" entitled to protection under Section 333, then the Part 15 device must also be a station for other purposes of Title III of the Act, a broad assertion which the Commission has never made and is unsupported by the history of unlicensed operations. Thus, to conclude that Part 15 devices are "stations" protected from interference under Section 333, would mean, by operation of law, that they could not be operated without the license called for in Section 307 and the Commission's entire "unlicensed" devices regulatory regime under Part 15 and other rules would be unlawful.

The distinction between unlicensed "devices" and licensed "stations" is hardly news to the Commission. Section 15.1 of the Commission's Rules makes clear that Part 15 sets out the "regulations under which an intentional, unintentional, or incidental radiator may be operated without an individual license" and that transmitting facilities not falling within the scope of Part

---

[27] *See* 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, 24589-91 (2004)("*UWB Reconsideration Order*")("In setting up the Part 15 regime, the Commission realized that any attempt to license all transmitters of radio frequency energy would be infeasible and contrary to Congress's intent in establishing a "rapid, efficient, Nation-wide, and world-wide wire and radio communication service." In this regard, the Commission has long recognized that numerous devices emit radio frequency energy, often at very low levels, and that such devices may be operated by numerous individual users, making individual licensing of users impractical. Recognizing that the identification and individual licensing of all devices that affected or relied upon radio frequency energy was not practical, the Commission, very early in its existence, interpreted Section 301 not to require the licensing of devices that did not transmit energy in a manner that had any real potential to affect the Nation's communications network adversely. In adopting this reading of the statute, the Commission recognized that many devices that operate at very low power levels and at very short distances are unlikely to cause harmful interference and thus would not need to be individually licensed.")(footnotes omitted).

15 "must be licensed pursuant to the provisions of section 301 of the Communications Act of 1934, as amended, unless otherwise exempted . . .."[28] The Part 15 rules do not authorize the operation of any "station".[29]

Moreover, Section 15.5 of the Rules subjects the operation of unlicensed devices "to the conditions that no harmful interference is caused and 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."[30] Presumably the Commission would not have listed Part 15 devices separate from "radio stations" if it believed that the term "radio stations" included Part 15 devices. Moreover, were Part 15 devices to fall within the definition of "radio stations" or "stations," then the provisions of Section 15.5(b) obligating Part 15 devices to accept interference from each other would contravene the protections of Section 333 protecting "stations" from interference. 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.[31]

---

[28] 47 C.F.R. § 15.5(b).

[29] Indeed, throughout Part 15 are rules that reflect the dichotomy between Part 15 "radiators" or "devices" and "stations" licensed under Title III. *See, e.g.* 47 C.F.R. § 15.5(b) (requiring "an intentional, unintentional or incidental radiator" to accept interference that may be caused "by the operation of an authorized radio station".); § 15.17 (cautioning Part 15 equipment designers "to consider the proximity and the high power of non-Government licensed radio stations" in selecting frequencies.).

[30] 47 C.F.R. § 15.15(b).

[31] Cisco recognizes that in decisions addressing Part 15, the Commission has on occasion referenced in its ordering clauses to, among numerous other provisions of the Act, Section 303 generally (which only references "stations" in subsection (f) or, more specifically, Section 303(f), which authorizes the Commission to "[m]ake such regulations not inconsistent with law as it may deem necessary to prevent interference between stations and to carry out the provisions of this Act," or,. *See, e.g.* Authorization of Spread Spectrum and Other Wideband Emissions Not Presently Provided for, *Further Notice of Inquiry and Notice of Proposed Rulemaking*, 98 FCC 2d 380, 396 [¶ 43] (1984) (citing §§ 4(i) and 303 generally); Operation of Unlicensed NII

The dichotomy between "devices" and "stations" inherent in Part 15 is appears to be grounded in Section 302 of the Act, which provides that "[t]he Commission may, consistent with the public interest, convenience, and necessity, make reasonable regulations (1) governing the interference potential of *devices* which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications . . . .[32] Section 302 of the Act and Part 15 of the Commission's Rules can only be read in harmony with Section 333 and the other provisions of Title III of the Act by acknowledging that "stations" are separate and distinct from "radiators" or "devices." To avoid undermining its entire unlicensed device regulatory regime the Commission should declare that Section 333 of the Act is inapplicable to Part 15 devices because they are not "stations" entitled to protection thereunder.

IV. THE COMMISION SHOULD ADOPT A POLICY STATEMENT REGARDING THE MANAGEMENT OF UNLICENSED SPECTRUM

Concluding that Section 333 does not apply to Part 15 devices also has the added benefit of allowing the Commission to establish policies that distinguish between "good" management practices and "bad" ones. Section 333 is absolute – willful or malicious interference is banned

---

Devices in the 5 GHz Frequency Range, *Memorandum Opinion and Order*, 13 FCC Rcd 14355, 14382 [¶ 63] (1998) (ordering clause citing §§ 4(i) 303(c), (f), (g), and (r); Review of Part 15 and Other Parts of the Commission's Rules, *Second Report and Order and Memorandum Opinion and Order*, 18 FCC Rcd 14741, 14766 [59] (2003) (ordering clause citing §§ 4(i), 301, 302, and 303(e), (f), and (r)); 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, 4164 [¶ 138] (2014) (ordering clause citing §§ 4(i), 301, 302, and 303(e), (f), (g) and (r)); *UWB Reconsideration Order*, 19 FCC Rcd at 24604 [¶105](ordering clause citing §§ 4(i), 302, 303(e), 303(f), 303(r), 304 and 307 of the Act). In none of those decisions, however, does the Commission engage in any analysis or otherwise suggest that Part 15 devices are "stations." Indeed, because these decisions reflected the general construct of Section 15.5(b) – Part 15 devices can not cause harmful interference and must accept interference – there is no basis to suggest from such fleeting and non-substantive references that the Commission intended to regulate Part 15 devices as "stations" that would be subject to Section 333 of the Act.

[32] 47 U.S.C. § 302 (emphasis added).

without regard to the motives of the party making the transmission. If containment through the sending of a deauthentication frame constitutes interference, then Section 333 is violated whether the sender is protecting its network from a security attack (which the Enforcement Bureau seems to recognize is a good use of deauthentication)[33] or is seeking to maliciously disrupt a neighbor's Wi-Fi use (which most would acknowledge is a bad use of deauthentication). Given that there is no Wi-Fi without deauthentication frames (or any other components of the 802.11 management frame system) the Commission cannot box itself in because it disapproves of the way in which deauthentication frames are used in a particular case. The Commission must distinguish between the transmission of network management frames, including deauthentication frames, and the purposes for which those frames are sent.

While the Hotel Petition suggests a rulemaking proceeding as a possible avenue for addressing the legitimacy of network management practices,[34] Cisco disagrees. Certainly, no one should not have *carte blanche* to disrupt the operation of Wi-Fi or other unlicensed devices without legitimate justification. However, it is both unwise and premature for the Commission to try to establish formal rules that would distinguish between permitted and banned network management practices.

The problem, simply stated, is that those who abuse Wi-Fi for illegitimate ends are clever and constantly devising new methods to take advantage of opportunities for wrongdoing. As a result, industry is constantly playing "catch up", reacting as new techniques for abuse are developed. As a result, it would be a mistake for the Commission to take a snapshot of the current situation and develop a comprehensive regulatory regime that could preclude industry from addressing new threats as they arise.

[33] Marriott Consent Decree at ¶ 6.

[34] *See* Hotel Petition at 19-21.

Thus, Cisco urges the Commission to issue a policy statement on Wi-Fi management (perhaps in the form of an Office of Engineering and Technology bulletin) 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. Because such a policy statement can be readily modified without the administrative requirements of a rulemaking proceeding, it will provide the Commission and its staff with the maximum flexibility to adjust to new developments over time.

The record developed in response to the Hotel Petition should serve as a useful starting point in the development of such a policy statement. For example, Cisco recommends that at a minimum a policy statement should encourage Wi-Fi network operators to only utilize IEEE 802.11 management frames to contain the operation of unmanaged or unauthorized Wi-Fi devices when doing so addresses security or other legitimate concerns such as those identified above. In doing so, the Commission should make clear that:

- The Part 15 regime is predicated on a set of conditions that allow all unlicensed transmitters to contend for spectrum resources. In general, in the absence of a security consideration (or in other limited cases), network administrators should not take actions that deny unlicensed transmitters use of spectrum.

- Use of active containment capability by a network administrator is strongly discouraged in environments where unlicensed networks are geographically clustered together unless an unmanaged or unauthorized transmitter is confirmed to be operating on premises and presents a security threat.

- If use of unlicensed ad hoc clients or personal hot spots is restricted for security reasons, such as federal government or critical infrastructure installations, the enterprise should endeavor to provide a clear and transparent disclosure to employees and contractors.

- Denial of spectrum resources in enterprise locations where the public is routinely invited or present, such as hotels, convention centers, airport terminals, is strongly discouraged in the absence of a security threat. The mere presence of a personal hot spot or ad hoc client does not constitute a security threat in any venue or physical location where the public is routinely present or invited.

A policy such as this would serve to put network administrators on notice that their behaviors in managing networks have a direct link to the law and regulations that permit unlicensed networks to exist. At the same time, the policy could be amended or expanded as factual cases present themselves before the Commission. Cisco urges the Commission to consider such a statement in lieu of a rulemaking. Moreover, before additional enforcement actions are taken on similar facts to the Marriott case, the Commission would be well-served to resolve this proceeding, and issue the recommended policy statement. This will put network administrators on notice, and permit them an opportunity to comply.

V. CONCLUSION

Rather than continue attempts to address unlicensed network management practices through *post hoc* Enforcement Bureau activity, the Commission should embrace the opportunity presented by the Hotel Petition to engage all of the Wi-Fi industry in a dialog regarding network management practices and to provide industry with additional clarity as industry grapples with the ever-escalating set of threats posed by Wi-Fi abuse. While, for the reasons set forth above, the Enforcement Bureau's reliance on Section 333 is misplaced, the Commission can and should issue a policy statement recommending best practices for balancing the Commission's goals for Wi-Fi with the needs of government agencies, educational institutions and other enterprises to maintain security and management Wi-Fi use for other legitimate purposes.

Respectfully submitted,

CISCO SYSTEMS, INC.

By: /s/ Mary L. Brown
Mary L. Brown

Director, Government Affairs
601 Pennsylvania Avenue, NW
9th Floor North
Washington, DC 20004
(202) 354-2923

December 19, 2014