Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

REPLY COMMENTS OF THE CONSUMER ELECTRONICS ASSOCIATION IN OPPOSITION TO PETITION FOR DECLARATORY RULING OR RULEMAKING

Property owners may not block the operation of Wi-Fi devices. The Consumer Electronics Association ("CEA")[1] opposes the petition of the American Hospitality & Lodging Association, Marriott International, Inc. and Ryman Hospitality Properties that seeks a declaratory ruling or, in the alternative, a rulemaking proceeding to the contrary.[2] End users – not property owners – possess the right to operate Wi-Fi devices. Third-party disruptions of that right are unlawful and contrary to the public interest.

---

[1] CEA is the principal U.S. trade association of the consumer electronics and information technologies industries. CEA's more than 2,000 member companies lead the consumer electronics industry in the development, manufacturing and distribution of audio, video, mobile electronics, communications, information technology, multimedia, and accessory products, as fihou3(s)-11.andA'sfef iionihe(f)-246.United(a)]TJT*.0009TcS(W)-6.t(C)-5.at(C)-5.ries.

The lodging industry maintains nearly 5 million guest rooms nationally[3] and more than 100 million Americans live in rental properties.[4] The ability of consumers and businesses to communicate and conduct their affairs using Wi-Fi data connections should not depend on whether individuals have ownership rights in locations in which they live, work or visit.

CEA thus opposes the Petition, along with the vast majority of the commenters in this proceeding, and urges the Commission to unambiguously hold that Wi-Fi devices are entitled to protection from willful and malicious interference under federal law, consistent with both the plain text of the Communications Act of 1934, as amended, and the Commission's longstanding interpretation of section 333 of the Act. Similarly, while there is a legitimate and pressing need for network management and security for Wi-Fi systems, the Commission should affirm that Wi-Fi operators may not transmit de-authentication frames to third-party Wi-Fi systems or devices. Network management and security practices are critical, but should be limited to an operator's own system, not the Wi-Fi systems of other service providers.

DISCUSSION

I. Part 15 Devices Are Entitled to Protection From Willful or Malicious Interference Under 47 U.S.C. § 333.

CEA supports the position of the vast majority of the commenters, including dozens of individual citizens, holding that Part 15 devices are entitled to protection from willful or malicious interference under 47 U.S.C. § 333.[5] The statute on its face extends protection to both

---

[3] American Hotel & Lodging Association, http://www.ahla.com/content.aspx?id=36332 (figure based on 2013 data) (last visited December 31, 2014).

[4] National Multifamily Housing Council, http://www.nmhc.org/Content.aspx?id=4708 (figure based on 2014 U.S. Census Bureau survey data) (last visited December 31, 2014).

[5] *See, e.g.*, Opposition of Google Inc. at 2 (Dec. 19, 2014); Comments of Microsoft Corporation at 1 (Dec. 19, 2014); Opposition of the National Cable & Telecommunications Association at 3-4 (Dec. 19, 2014); Comments of CTIA–The Wireless Association at 3-5 (Dec. 19, 2014);

licensed and authorized radio stations.[6] Wi-Fi devices are authorized unlicensed equipment operating pursuant to Part 15 of the Commission's rules and, accordingly, qualify for protection under the statute.[7]

There is no basis to conclude, as the Petitioners and others argue, that Wi-Fi devices are not "stations" subject to protection under 47 U.S.C. § 333.[8] The Commission's rules, which are based on the International Telecommunication Union Radio Regulations ("ITU RR"), broadly define a station as "one or more transmitters or receivers or a combination of transmitters and receivers . . . necessary at one location for carrying on a radiocommunication service."[9] A radiocommunication service is defined as "[a] service as defined in this Section involving the transmission, emission and/or reception of radio waves for specific telecommunication purposes."[10] Wi-Fi devices are comprised of both a transmitter and receiver and use radio waves to provide fixed two-way data communications and, accordingly, readily meet this definition.[11]

Opposition of Open Technology Institute at New America Foundation and Public Knowledge to Petition for Declaratory Ruling or, in the Alternative, For Rulemaking at 4-5 (Dec. 19, 2014); Opposition of the Wireless Internet Service Providers Association to Petition for Declaratory Ruling or, in the Alternative, For Rulemaking at 4-5 (Dec. 19, 2014).

[6] 47 U.S.C. § 333 ("No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station *licensed or authorized* by or under this chapter or operated by the United States Government.")(emphasis added).

[7] Wi-Fi devices also must comply with Part 2 of the FCC's rules regarding equipment authorizations. *See* 47 C.F.R. §§ 2.901 *et seq*.

[8] *See, e.g.*, Petition at 16; Joint Comments of Aruba Networks, Inc. and Ruckus Wireless, Inc. at 9 (Dec. 19, 2014); Comments of Smart City Networks, LP at 8-9 (Dec. 19, 2014).

[9]

The Commission has also stated repeatedly that Wi-Fi devices are entitled to interference protection under 47 U.S.C. § 333.[12] For example, the Commission recently released an Enforcement Advisory reminding the public that operation of devices that block, jam or otherwise interfere with radio communications, including devices that "prevent . . . [a] Wi-Fi enabled device from connecting to the Internet" are illegal.[13] Moreover, the Commission has previously taken action to prevent interference to unlicensed devices in other contexts. For example, in 1995, as part of a rulemaking proceeding to establish a new Location and Monitoring Service ("LMS"), operating in the 902-928 MHz band, the Commission established a rule designed to protect co-channel Part 15 devices by requiring licensees, as a license condition, to "demonstrate through actual field tests that their systems do not cause unacceptable levels of interference to Part 15 devices."[14]

"harmful interference" to other Part 15 devices and not that Part 15 devices must suffer willful or malicious interference. *Cf. Continental Airlines Petition for Declaratory Ruling Regarding the Over-The-Air Reception Devices (OTARD) Rules*, Memorandum Opinion and Order, 21 FCC Rcd 13201 (2006) (concluding that Wi-Fi signals are "fixed wireless signals" subject to the OTARD rules).

[12] *See, e.g*

The Commission also has taken the position that Wi-Fi systems are protected under the Over-The-Air Reception Devices ("OTARD") rules.[15] The OTARD rules were implemented to ensure that property owners could not impede access to new technologies or inhibit competition.[16] These same reasons support the conclusion that the interference protection of section 333 applies to Wi-Fi devices and refute the Petitioners' arguments that such a conclusion is inconsistent with the OTARD rules.[17]

II. Wi-Fi Operators May Manage the Network and Security of Their *Own* Wi-Fi Systems, But Not the Systems of Others

The recent data breaches of major international corporations highlight the importance of implementing strong cyber security measures for data networks.[18] The President has also stated

---

[15] *Continental Airlines Petition for Declaratory Ruling Regarding the Over-The-Air Reception Devices (OTARD) Rules*, Memorandum Opinion and Order, 21 FCC Rcd 13201 (2006).

[16] *See, e.g., Preemption of Local Zoning Regulation of Satellite Earth Stations and Implementation of Section 207 of the Telecommunications Act of 1996, Restrictions on Over-The-Air Reception Devices: Television Broadcast Service and Multichannel Multipoint Distribution Service*, Report and Order, 11 FCC Rcd 19276 ¶ 6 (1996) ("The rule is designed to promote two complementary federal objectives: (a) to ensure that consumers have access to a broad range of video programming services, and (b) to foster full and fair competition among different types of video programming services."); *Promotion of Competitive Networks in Local Telecommunications Markets*, First Report and Order and Further Notice of Proposed Rulemaking, Fifth Report and Order and Memorandum Opinion and Order, Fourth Report and Order and Memorandum Opinion and Order, 15 FCC Rcd 22983 ¶¶97-100 (2000) (expanding OTARD rules to apply to fixed wireless signals and to include voice and data services).

[17] Petition at 18-19. CEA also disputes the Petitioners' blanket statement that hotel guests "are at most invitees or licensees," having no rights under the OTARD rules. *Id*. at 19. For example, generally under California law, residents of hotels and motels that have resided in a hotel or motel for longer than 30 days have the same legal rights as tenants. *See* Ca. Civil Code § 1940(a); *see also* California Department of Consumer Affairs, http://www.dca.ca.gov/publications/landlordbook/whois.shtml.

[18] *See, e.g*., Danny Yadron, Wall Street Journal, "Corporate Boards Race to Shore Up Cybersecurity" (Jun. 29, 2014), *available at* http://www.wsj.com/articles/boards-race-to-bolster-cybersecurity-1404086146

that "[i]t is the policy of the United States to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."[19] Accordingly, CEA recognizes that there is a legitimate and pressing need for network management and security of Wi-Fi systems.[20]

While a Wi-Fi operator could block access to *its own system* by unauthorized devices, section 333 of the Communications Act prohibits an operator from blocking access of devices to *other Wi-Fi systems*.[21] Many of the practices that the Petitioners propose to be sanctioned by the Commission fall into the latter category.[22] Moreover, practices that involve knowingly transmitting false information to third-party devices raise questions about possible violations of section 303(m)(1)(D)(1) of the Communications Act, as amended.[23]

---

http://www.reuters.com/article/2014/05/16/us-cyber-summit-infrastructure-idUSBREA4F0OK20140516.

[19] *See* "Improving Critical Infrastructure Cybersecurity," Executive Order No. 13636, 78 FR 11739 (Feb. 19, 2013).

[20] .l3.nt6art8(e)5.ut8(e)5.tNeeeNiteeb.6406-031mm739 (F4.5(i])-7.5(t)-24e1(m)-2.2cecati6notett09T[(l440127(n

There are alternatives to the network management and security practices proposed by Petitioners. For example, with respect to access point spoofing or "honey pot" attacks, informing consumers or guests about proper log-in procedures and providing the correct information regarding the authorized Wi-Fi network could defuse such threats.[24] Similarly, with respect to corporate or educational institution policies prohibiting unauthorized Wi-Fi use, property owners could implement a rule prohibiting such devices on the premises, as the Petitioners themselves concede.[25] Quite apart from the intrinsic benefits of free expression and fairness associated with allowing consumers to choose their preferred source of Wi-Fi connectivity based on their needs and budget, consumer education will generate more reliable, cost-effective, and secure network data connections more often and more consistently than would allowing property owners to serve as the arbiters of consumer broadband consumption that happens to occur on the owners' premises.**cconsumer4.3(r)(824.6)343.59III.Tm162554.7TD3.6(-)251.itfmotern**

same functionality, ensuring that consumers have ubiquitous Internet connectivity.[27] Similarly, mobile operators have deployed Wi-Fi networks to decrease congestion on licensed cellular networks,[28] and fixed broadband providers have done so to offer enhanced functionality of their own service offerings.[29]

affairs using Wi-Fi data connections should not depend on whether individuals have ownership

may not transmit de-authentication frames to third-party Wi-Fi systems or devices located on the operator's property.

Respectfully submitted,

CONSUMER ELECTRONICS ASSOCIATION

By: *_/s/ Julie M. Kearney_*

Julie M. Kearney
Vice President, Regulatory Affairs
Brian E. Markwalter
Senior Vice President, Research and Standards
Consumer Electronics Association

CERTIFICATE OF SERVICE

I, Deborah Johnson, hereby certify that on January 5, 2015, a true and correct copy of these Reply Comments was sent via U.S. Mail, first class postage prepaid, to the following:

Bennett L. Ross
David Hilliard
Henry Gola
Wiley Rein LLP
1750 K Street, NW
Washington, DC 20006
Counsel for Marriott International and Ryman Hospitality Properties

Banks Brown
McDermott Will & Emery LLP
340 Madison Avenue
New York, NY 10174-1922
Counsel for the American Hospitality & Lodging Association

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

Scott Maples
Vice President, General Counsel
Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089

Marta Beckwith
Vice President, Legal
Aruba Networks
1344 Crossman Avenue
Sunnyvale, CA 94089

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

Michael Daum
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

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

Peter Tannenwald
Fletcher, Heald & Hildreth, PLC
1300 N. 17th Street, 11th Floor
Arlington, VA 22209-3801
Counsel for Brown University

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

Mark E. Crosby
President/CEO
Enterprise Wireless Alliance
2121 Cooperative Way, Ste. 225
Herndon, VA 20171

Mark Haley
President

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

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

Michael F. Altschul
Scott K. Bergmann
Brian M. Josef
CTIA – The Wireless Association
1400 16th Street, NW, Suite 600
Washington, DC 20036

Rick Chessen
Neal M. Goldberg