Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 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

STATEMENT OF AD HOC TELECOMMUNICATIONS USERS COMMITTEE IN SUPPORT OF PETITION FOR DECLARATORY RULING OR, IN THE ALTERNATIVE, FOR RULEMAKING

The Ad Hoc Telecommunications Users Committee ("Ad Hoc") respectfully submits its statement in support of the above-captioned Petition for Declaratory Ruling or, in the Alternative, for Rulemaking ("Petition") filed by the American Hotel & Lodging Association ("AHLA"), Marriott International, Inc., and Ryman Hospitality Properties (collectively, "Petitioners").

The issues raised by the Petition are important not only to the hospitality industry, which Petitioners represent, but to the wide variety of businesses in other industries that operate wireless local area networks ("WLANs") on their premises.[1] In light of recent

[1] For over thirty years, the Ad Hoc Telecommunications Users Committee has represented enterprise customers in FCC proceedings that affect the services on which they rely. Ad Hoc members come from a broad range of industry verticals, including banking, construction, financial services, insurance, information services, logistics, manufacturing, payment processing, and systems integration. None of the Petitioners is a member of Ad Hoc.

uncertainty regarding the law and regulatory policies applicable to these technologies, Ad Hoc supports the initiation of a rulemaking in order for the Commission to develop a robust factual record on the basis of which it can then establish clear, generally applicable standards and policies.

The Petition describes the importance to hotels and other hospitality providers of ensuring the security and reliability of their Wi-Fi networks in order to preserve high-quality broadband wireless access to the Internet for guests. It describes a number of security threats to such networks as well as the reliability issues that can arise when numerous Part 15 devices occupy the airwaves in a circumscribed physical area. Among the specific threats it discusses are signal interception, unauthorized network access, unauthorized access points, and access point spoofing (also known as "honey pot" attacks).[2]

The Petition notes that in order to address these threats and others like them, WLAN operators can avail themselves of various network management measures that use certain built-in capabilities of the WLAN equipment the Commission has approved under Part 15 of its rules. The Petition asks the Commission to issue a declaratory ruling or commence an industry-wide rulemaking to clarify what WLAN operators may and may not do in deploying these measures.

Ad Hoc agrees that the Commission should address these issues in a manner that clarifies the rules for WLAN operators not only in the hospitality industry but in all industry sectors and commercial settings in which the equipment may be used. Those

---

[2] *See* Petition at 6-8.

settings are many and various. For example, retail stores may allow patrons on their premises to access their Wi-Fi networks, both to provide in-house content and to allow patrons to access the Internet in store areas where cellular reception may be spotty (or to allow them to shop online without using up their data plans). Transportation hubs such as airports and train or bus terminals may operate Wi-Fi networks to allow travelers to access the Internet during waiting times. Healthcare facilities may use WLANs to allow medical personnel to quickly access medical records and other key information from bedsides. Colleges and universities may offer students, faculty, and staff campus-wide wireless Internet access. And enterprise customers like the members of Ad Hoc may use their WLANs not only for their own employees but to facilitate network and Internet access for on-site visitors and vendors.

As the Petition points out, Part 15 devices commonly deployed by such users (and approved by the Commission) now have built-in, standard capabilities that allow them to recognize, and in many cases remedy, security issues that, if left unaddressed, would potentially allow massive incursions into private personal information or sensitive corporate data. Similarly, these capabilities allow network managers to mitigate reliability issues that could cause their networks to grind to a halt.

But recent Commission proceedings have provided confusing and inconsistent guidance regarding the circumstances in which users may reasonably rely on these capabilities to manage their networks without running afoul of Commission rules or the Communications Act. In some proceedings, the Commission has seemed to recognize clearly that reasonable network management is permitted by Commission rules, and in particular does not violate Section 333 of the Communications Act, which prohibits

"willful[] or malicious[]" interference.[3] In other proceedings, however, the Commission has taken the position that some management measures which utilize built-in, standard capabilities of Commission-approved equipment may constitute "interference" prohibited by Section 333.[4]

Customers of WLAN equipment need the Commission to establish clear rules and policies regarding what they may and may not do to manage their networks so as to mitigate growing security and reliability threats. Customers already face significant challenges in their efforts to fend off the ever-evolving efforts of hackers and network intruders and to address growing congestion issues, without additional uncertainty as to whether the Commission will subsequently find that such measures violate Commission policies or Section 333. Accordingly, Ad Hoc urges the Commission to initiate a comprehensive rulemaking proceeding in order to assemble a fulsome record on these issues and develop informed, clearly-written rules and policies that will enable end users to determine which practices are lawful and which are not.

For the foregoing reasons, Ad Hoc supports the commencement of a rulemaking to address the issues identified above and in the Petition.

Respectfully submitted,

AD HOC TELECOMMUNICATIONS USERS COMMITTEE

By: Colleen Boothby

[3] *See, e.g., Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, Notice of Proposed Rulemaking*, FCC 13-58, 28 FCC Rcd 6603 (2013); *Expanding Access to Mobile Wireless Servs. Onboard Aircraft, Notice of Proposed Rulemaking,* 28 FCC Rcd 17132, 2013 FCC LEXIS 4861 (2013).

[4] *Marriott International, Inc., Order,* File No. EB-IHD-13-00011303, DA 14-1444, rel'd Oct. 3, 2014.

Colleen Boothby
Levine, Blaszak, Block & Boothby, LLP
2001 L Street, NW, Ninth Floor
Washington, D.C. 20036
202-857-2550

Counsel for
Ad Hoc Telecommunications
Users Committee

December 19, 2014

Certificate of Service

I, Michaeleen Terrana, hereby certify that true and correct copies of the foregoing "Statement of Ad Hoc Telecommunications Users Committee in Support of Petition for Declaratory Ruling, or, in the Alternative, for Rulemaking" were served by first-class U.S. mail, postage prepaid, on the following:

Banks Brown
McDermott Will & Emery LLP
340 Madison Avenue
New York, NY 10174-1922

Counsel for the American Hospitality & Lodging Association

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

By:_____