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

In the Matter of	)	
	)	
Petition of 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	)	

COMMENTS IN OPPOSITION OF AMERICAN HOTEL & LODGING ASSOCIATION PETITION FOR DECLARATORY RULING OR, IN THE ALTERNATIVE, FOR RULEMAKING

Mark Saurman
Amateur Radio Licensee N8TLV
755 Sparrow Way
Wadsworth, OH 44281-7718

December 26, 2014

TABLE OF CONTENTS

PAGE

I. INTRODUCTION AND SUMMARY……2

II. ARGUMENT……3

III. CONCLUSION……..5

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

In the Matter of	)	
	)	
Petition of 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	)	

COMMENTS IN OPPOSITION OF AMERICAN HOTEL & LODGING ASSOCIATION PETITION FOR DECLARATORY RULING OR, IN THE ALTERNATIVE, FOR RULEMAKING

I. INTRODUCTION AND SUMMARY

I, Mark Saurman, as a concerned citizen and FCC licensed amateur radio operator respectfully request the FCC to rule against the suggestions of the petition of American Hotel & Lodging Association, Marriott International, Inc. (hereinafter referred to as "Marriott"), and Ryman Hospitality Properties (hereinafter referred to as "Ryman").

Marriott and Ryman make unreasonable comparisons to justify their assertions and furthermore the use of the equipment they cite to commandeer the airwaves for their own pecuniary interests may result in unlawful operation as the rules and regulations stand today.

Allowing the use of Title 47 of the Code of Federal Regulations Part 15 (hereinafter referred to as "Part 15") wireless equipment to utilize subterfuge to prevent the authorized use of wireless spectrum in order to "protect" the equipment operator's own use of the spectrum is analogous to a target distributed denial of service attack to legitimate sites on the internet so that the perpetrator could have more bandwidth to their self. Such action would set a precedent that willful and malicious interference to both licensed and legal unlicensed users is acceptable provided it is done under the guise of security.

Part 15 spectrum is meant to be shared by all, not monopolized by a corporation. If Marriott and Ryman would like to have exclusive bandwidth, they should apply for a licensed block of spectrum to use. If security is their concern, more robust security can be achieved via software means with methods such as VPN. It should also be noted that Marriott and Ryman, along with the equipment manufacturer Aruba Networks who filed comments in support of Marriott and Ryman all stand to profit financially from the actions suggested in the petition.

II. ARGUMENT

First and foremost, a consideration which was not addressed by Marriott and Ryman is that at least part of the spectrum in which the Aruba Networks equipment operates is shared with the Part 97 Amateur Radio Service, part of which the Amateur Service is a primary user. Part 97 users may use the same 802.11 wireless local area networking specifications as Part 15 and the equipment is interoperable with each other. However unlicensed Part 15 users may not communicate with licensees operating under Part 97 as this would be a violation of 47 CFR 301. Conversely licensees operating under Part 97 may not communicate with unlicensed stations as this would be a violation of 47 CFR 97.111(a)(1). The Aruba Networks equipment has not demonstrated an ability to differentiate from Amateur Radio Stations operating under Part 97 and unlicensed Part 15 users. If the equipment were to communicate with Part 97 users, this would constitute a violation. Furthermore, the equipment sends out data packets with falsified information which could clone a Part 97 user. This would cause the operator of the Aruba Networks equipment to not operate under Part 15 but the regulations of Part 97. Corporations would be prohibited to participate in such communications, even if licensed in the Amateur service as this is prohibited by 47 CFR 97.113(a)(2). Also, if the Aruba Networks equipment obstructs communication between licensed Amateur Radio stations then this is considered to be harmful interference. Harmful interference is defined in 47 CFR 97.3(a)(23) as, "Interference which…seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating in accordance with the Radio Regulations."

Arguments put forth by Marriott and Ryman make some unfair comparisons to other Part 15 devices such as cordless phones, baby monitors, and garage door openers. While there is no regulatory protection to Part 15 devices from interference, most of the aforementioned devices incorporate measures so that they don't interfere with each other or can attempt to escape interference if experienced, especially in the case of modern devices. Also, none of these devices are specifically manufactured to prevent the operation of other devices in order to improve its own operation. In fact, cordless phones are increasingly moving into the UPCS band where they are regulated by 47 CFR 15.323(c) to verify that the intended operating frequency and timeslot is not already in use by another device before transmitting, effectively preventing other UPCS users from interfering with each other. It is clear that with the increased proliferation of wireless devices that modern rulemaking takes the protection of other users, licensed and unlicensed, into account. Willful and malicious interference to any user should be prohibited.

Marriott and Ryman make the case that the presence of other Wi-Fi users can create a negative experience for their guests who pay them for service. One supporting argument is that other Wi-Fi users can impact the bandwidth available to their users. While this may be true, it's not only Wi-Fi which utilizes the 2.4 GHz spectrum. Cordless phones, Bluetooth devices, microwave ovens, and the presence of human beings themselves can all cause signal degradation and attenuation, thus negatively affecting bandwidth and quality. One has to wonder if all of these "unauthorized" users instead purchased Wi-Fi access through Marriott and Ryman's properties if they would still be adverse to the impact these users would have on the overall availability of bandwidth. The nature of this spectrum should dictate that the continuous attainment of the maximum possible technical specifications cannot be guaranteed. Users should either be directed to a wired solution or Marriott and Ryman should apply to license spectrum for exclusive use of which they can provide equipment to guests on a loaner basis. Another negative aspect is the potential for security threats. Instead of attempting to address only access points which mimic their own, they treat every access point other than theirs as hostile, employing technical measures to block connectivity to them. While seeking to protect their Wi-Fi reliability, they want to reduce the reliability of every other connection within range. There are ways of mitigating security risks without negatively impacting others use of the spectrum. For example, free open source VPN solutions are available which could provide a secure pipeline to their network. If allowed, their same method of denying others access to other networks could be exerted upon them. Then no devices would be able to connect to any access points.

Marriott and Ryman go on to make the comparison of their proposed active monopolization of Wi-Fi to measures imposed by universities on their users who abuse their network such as bandwidth caps and throttling. In the case of all of the examples put forth in Marriott and Ryman's extensive appendix, all of these network management techniques are placed on users of their network, not on users of other networks within radio range. As users of their network, they must adhere to the rules and regulations imposed by the provider. The provider does not have the right to apply these rules and regulations to anyone else. The comparisons are therefore irrelevant and their point is moot.

Attacking access points can also negatively impact security. Any residence or business within Wi-Fi range of the Aruba Networks device could have their Wi-Fi security cameras or security system rendered inoperable. Users of a private network with devices such as an Apple iPod Touch could not use their device send text messages or make a VoIP call in the case of an emergency situation.

III. CONCLUSION

Based on the aforementioned arguments, the Commission should deny the petition put forth by Marriott and Ryman. A Wireless Network Operator does have the right to administer their own network, however this right is not transferrable onto other networks. An individual, Wi-Fi Network Operator or otherwise, should not have the right to cause deliberate, harmful interference to other users. Marriott and Ryman have not displayed the ability to ensure with one hundred percent confidence that their mitigation efforts would never affect anyone outside of their numerous properties. They have not demonstrated the ability to protect licensed 802.11 users of Wi-Fi frequencies. They have not demonstrated that the act of spoofing deauthorization packets is the only effective method of ensuring guest bandwidth and security. This is because alternatives do exist. Instead they wish to monopolize Wi-Fi to force users onto their pay structure to pad their bottom line. I urge the Commission to rule against what amounts to unfair business practices at the least and affirm such practice is a violation of the law which protects Radio Amateurs.

Respectfully,

Mark Saurman
Amateur Radio Licensee N8TLV
755 Sparrow Way
Wadsworth, OH 44281-7718