

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 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 KARL KOSCHER

I am submitting these comments in my capacity as an individual. As background, I recently received a Ph.D. in computer science (specializing in security) from the University of Washington and hold an amateur radio technician license. While other commenters have quibbled over legal definitions, I believe there are some higher-level problems with the Petitioners’ arguments. In particular, while the Petitioners argue that they are simply managing *their* networks and protecting users from security threats, I believe these arguments are somewhat disingenuous.

The “Petitioners request that the Commission declare that the operator of a Wi-Fi network does not violate Section 333 by using FCC-authorized equipment to monitor and mitigate threats to the security and reliability of its network.”¹ However, the Petitioners seek authorization to use technological means (deauthentication frames) to interfere with “unauthorized” access points that are *not* part of their network. The mere fact that multiple networks are co-located does not make them part of the same network. As the Petitioners point out, several universities have set out policies for use of their wireless network. However, none of the policies cited affect users of *other* networks, including those co-located with official campus networks, which makes their inclusion in the Petition puzzling.

An argument may be made that limiting “unauthorized” access points is required to ensure network performance. However, as Part 15 devices, WiFi devices are not protected against harmful

¹ Petition at 3

interference, such as packet collisions from other WiFi devices. Allowing users of Part 15 devices to *intentionally* interfere with others in order to minimize their own interference appears to fly in the face of long-standing Part 15 policy. Furthermore, it is unclear whether over-the-air interference is actually the bottleneck in network performance at the Petitioners' venues. Anecdotally, the Internet uplink at conference venues has often been the bottleneck, with even wired users suffering from poor performance.

Even if spectrum congestion is a problem, it is unclear how much limiting "unauthorized" access points helps. For example, if a user is downloading a file, those packets must go over the air, whether it is from the venue's access points or their own personal "hotspot." It is even plausible that personal "hotspots" reduce congestion—being closer requires less power and may yield a higher signal-to-noise ratio, which allows use of more advanced and time-efficient modulation schemes. It should be noted that at the annual DEFCON conference (one of the world's largest "hacker" conventions and considered by many to have the "most hostile network on earth"), WiFi performs extremely well, despite hundreds of paranoid attendees using their own personal "hotspots," while others download large files from the network's media server from the venue's official network.

Allowing property owners to interfere with private WiFi networks wouldn't necessarily improve spectrum congestion, and in fact may be counter-productive. While WiFi is perhaps the most popular application of the 2.4 GHz, it is by no means the only application. For example, many Android phones support tethering over WiFi *and* Bluetooth. If a venue actively interferes with tethering over WiFi, users may choose to tether over Bluetooth, which may cause significantly more interference due to the differences between WiFi and Bluetooth technologies.

If spectrum congestion is truly a concern, the Commission could potentially license additional protected spectrum. This spectrum could either be WiFi channels that are currently unavailable in the U.S. but nonetheless supported by many WiFi network adapters, or new dedicated spectrum (such as the 3.6 GHz band).

Finally, the Petitioners also argue that interfering with "unauthorized" access points is necessary to protect their users from security threats. However, this claim seems overstated. WiFi provided by

venues is almost always provided unencrypted. In contrast, most personal “hotspots” use the latest WPA2 WiFi encryption technology. Interfering with these “unauthorized” personal networks forces users to fall back to less secure networks. It is relatively straight-forward for a malicious actor to sniff unencrypted WiFi even if their network card is not “associated” with the network.

While enterprise WiFi equipment often has protections built in that isolate “associated” users from each other (and thus preventing a malicious user from attacking another), these protections can be bypassed on unencrypted networks at the physical layer by “spoofing,” or impersonating, the legitimate access point. This impersonation can happen either at the access point level (by impersonating the SSID) or at the frame level (by injecting a packet over the air). While interfering deauthentication frames can protect users against access points with impersonated SSIDs, they cannot protect them from “spoofed” frames (although these attacks are harder to execute). *If* the Commission were to agree to allow network operators to use interfering deauthentication frames on a limited basis, it should be *solely* to prevent the use of “rogue” access points that impersonate the SSID of another network. It should be noted that there may be other means to address “rogue” access points, including radio direction-finding/geolocation (which is mentioned in the Petition as a way to prevent the proposed “management” techniques from interfering with WiFi devices outside of a venue.)

In summary, the justifications made the Petitioners are thin, and in my opinion, seem like excuses to squeeze more revenue out of conference organizers and attendees. The Petitioners could discourage the use of “unauthorized” access points by making their networks more competitively-priced and performant. Instead, they seek a monopoly on the local 2.4/5 GHz spectrum in order to charge arbitrary rates for access to their networks. This is a radical departure from the spirit, if not the letter, of the Part 15 rules, which the Commission should clearly reject.

Respectfully submitted,

/s/ Karl Koscher