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 SIRENGPS CORPORATION

Marriott International, Inc., Ryman Hospitality Properties, and the American Hotel & Lodging Association (collectively, "Hotel Industry Interests," or "Petitioners") have asked the Federal Communications Commission ("FCC" or "Commission") to rule "that the operation of FCC-authorized equipment by a Wi-Fi operator in managing its network on its premises does not violate 47 U.S.C. § 333, even though it may result in interference with or cause interference to a Part 15 device being used by a guest on the operator's property."[1] SirenGPS urges the Commission to reject the Petition.

I. INTRODUCTION AND SUMMARY

The plain wording of the Communications Act of 1934, as amended ("Communications Act" or "Act") precludes the relief that the Hotel Industry Interests seek. Specifically, Section 333 is simple and straightforward: "No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under

[1] 1*Petition of the American Hospitality & Lodging Association, Marriott International Inc., and Ryman Hospitality Properties for Declaratory Ruling to Interpret 47 U.S.C. § 333, or, in the Alternative, for Rulemaking*, RM-11737 at 1 (filed Aug. 25, 2014) ("Petition").

this chapter or operated by the United States Government."[2] The statute does not provide for the exceptions sought by the Hotel Industry Interests. Because transmissions by Part 15 devices constitute authorized radio communications, unlicensed Wi-Fi operations are protected by Section 333. The Wi-Fi network "management" for which Petitioners seek authorization would be a conscious and deliberate act that exploits Wi-Fi operating protocols to interfere with authorized radio communications and would therefore be willful,[3] as proscribed by the Act. The Commission should also reject the Hotel Industry Interests' alternative request that the Commission initiate a rulemaking to amend its Part 15 rules "to specify the interference to Part 15 devices that Section 333 prohibits."[4] There is no inconsistency between the Commission's Part 15 rules and Section 333 with respect to interference to unlicensed devices that warrants a rulemaking. While a Part 15 device must accept interference from other devices, including Part 15 devices, interference to that device cannot be caused willfully.

The Commission has made it clear that "it is illegal to use a cell phone jammer or any other type of device that blocks, jams, or interferes with authorized communication."[5] The Hotel Industry Interests argue that the "Petition does not involve signal jammers."[6] While true, it is irrelevant, as the Commission considers "jammers" to be a broader range of devices "that are designed to block, jam, or otherwise interfere with authorized radio communications."[7] For example, consumers may wish to use so-called "Mi-Fi" devices to convert their

---

[2] 47 U.S.C. § 333.

[3] *See* 47 U.S.C. § 312(f) (defining "willful" as "the conscious and deliberate commission or omission of [an] act, irrespective of any intent to violate any provision of this Act or any rule or regulation of the Commission").

[4] *See* Petition at 19.

[5] *FCC Enforcement Advisory: WARNING: Jammer Use is Prohibited*, Enforcement Advisory No. 2014-05, Public Notice, DA 14-1785, 2014 FCC LEXIS 4575 (2014) ("2014 Enforcement Advisory").

[6] *See* Petition at 3.

[7] 2014 Enforcement Advisory.

personal mobile devices into Wi-Fi access points. Both the Mi-Fi dongle and the consumer's personal device contain Part 15 radios. Sending radio transmissions that de-authenticate the packets needed to associate these two Part 15 devices "interferes with" the operation of these authorized devices. Although not the same as a signal jammer that causes "interference to" a Mi-Fi station's receiver, both result in the same outcome and thus violate Section 333. While the technology behind Wi-Fi de-authentication can be used for legitimate purposes, a willful use of that technology to "jam" or otherwise interfere with Part 15 devices violates Section 333.

II. ARGUMENT

A. Part 15 Devices Are Protected as "Authorized" Devices Under Section 333.

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 chapter or operated by the United States Government."[8] Fatal to the Petition, these protections are not limited solely to "licensed" stations, but include communications of authorized stations. The Commission's Part 15 rules establish "the regulations under which an intentional, unintentional, or incidental radiator may be operated without an individual license."[9] While a person does not have to obtain a license to use a Part 15 transmitter, the transmitter itself is required to have an FCC authorization before it can be marketed legally in the United States.[10] By requiring such an authorization, the Commission helps ensure that Part 15 devices comply with its technical standards and, consequently, are capable of being operated with much lower

[8] 47 U.S.C. § 333.
[9] 47 C.F.R. § 15.1(a).
[10] *See* 47 C.F.R. §§ 15.201(b) and 2.803(b).

risk of causing interference to licensed operators. Because they all must meet the Commission's standards in order to be marketed, Part 15 devices are "authorized" within the meaning of Section 333.

None of the other terms in Section 333 suggest any difference in the protection for licensed and unlicensed devices. The statute prohibits willful interference with "any radio communications" of "any [radio] station." The definition of "radio communication" covers the operations of Wi-Fi hotspots, which operate through "the transmission by radio of writing, signs, signals, pictures, and sounds of all kinds, including all instrumentalities, facilities, apparatus, and services (among other things, the receipt, forwarding, and delivery of communications) incidental to such transmission."[11] A "radio station" is "a station equipped to engage in radio communication or radio transmission of energy."[12]

Moreover, the term 'interference" as defined in the Commission's rules also does not differentiate between licensed and unlicensed use. Interference is defined as "[t]he effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy."[13] A de-authentication packet transmitted by a hotel's network to the consumer's Wi-Fi hotspot has the precise effect, as intended by its sender, of preventing the consumer from using the hotspot to send and receive "information which could be extracted in the absence of such unwanted energy."[14]

---

[11] 47 U.S.C. § 153(40).
[12] 47 U.S.C. § 153(42).
[13] 47 C.F.R. § 2.1.
[14] *Id.*

B. <u>Use of Authorized Devices to Willfully Interfere With a Consumer's Authorized Device Violates Section 333.</u>

The Petitioners do not deny that the use of their "network management systems" against consumers' Wi-Fi hotspots are intentional acts.[15] The term "willful" is defined as "the conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate any provision" of the Communications Act.[16] The management of a Wi-Fi network is a conscious and deliberate act, and using network management equipment to interfere with authorized radio communications for the purpose of preventing those communications, regardless of the rationale, is therefore also willful conduct proscribed by Section 333.

The Commission has made clear on numerous occasions that intentional interference with unlicensed devices violates Section 333,[17] and that its definition of "jammers" includes devices used to intentionally prevent others' Wi-Fi connections.[18] A person who uses FCC-authorized equipment to de-authenticate another device interferes with that device's operation by preventing it from attaching to its desired access point. Similarly, a person willfully operating a device to fill the air with energy, in the form of noise, a discernable signal, or beacons, for purposes of reserving the medium, and preventing a Wi-Fi device from attaching to an access point in a

---

[15] *See, e.g.*, Petition at 8 (stating that "hotels have purchased and installed network management systems . . . that allow a hotel to manage its Wi-Fi networks").
[16] *See* 47 U.S.C. § 312(f).
[17] *See* 2014 Enforcement Advisory (stating that a device that "prevents your Wi-Fi enabled device from connecting to the Internet" "interferes with authorized radio communications"); *FCC Enforcement Advisory: Cell Jammers, GPS Jammers, and Other Jamming Devices*, Enforcement Advisory No. 2012-02, Public Notice, DA 12-1642, 27 FCC Rcd. 2309 (2012) (same); *FCC Enforcement Advisory: Cell Jammers, GPS Jammers, and Other Jamming Devices*, Enforcement Advisory No. 2011-04, Public Notice, DA 11-250, 26 FCC Rcd. 1329 (2011) ("We remind consumers that it is a violation of federal law to use devices that intentionally block, jam, or interfere with authorized radio communications such as cell phones, police radar, GPS, and Wi-Fi.").
[18] *See, e.g.*, *id.*

geographic area for an indeterminate period of time would also implicate Section 333.

The Hotel Industry Interests seek to use the FCC's authorization of its network management equipment under Part 15 to bootstrap its erroneous argument that Section 333 does not protect unlicensed devices against willful interference from the use of other Part 15 devices. First, Petitioners point out that, unlike "signal jammers," network management systems serve other purposes and are authorized by the Commission.[19] However, authorized devices can also be used to willfully interfere with or cause interference to authorized devices. The dispositive factor under Section 333 is how the device's technology is being used. Petitioners' speculated "absurd results" and "illogical consequences" disappear once the willfulness requirement of Section 333 is brought into focus.

Second, the Hotel Industry Interests' argument conflates the hotels' management of their own networks with the hotels' attempt to effectively enclose the unlicensed spectrum around its facilities against other authorized Part 15 devices. Petitioners submit that Wi-Fi network operators should be able to use FCC-authorized equipment to monitor and mitigate threats to the security and reliability of their networks. Microsoft agrees that Wi-Fi network operators should be permitted to use FCC-authorized equipment to monitor their own networks. However, a Wi-Fi hotspot generated by a consumer's mobile phone is not part of the hotel's network, and is also authorized to operate in the unlicensed spectrum. Willfully excluding these other authorized devices from using that unlicensed spectrum, under the guise of mitigating so-called threats to the reliability (performance) of an operator's own network, violates Section 333.

Likewise, a Wi-Fi operator's interest in mitigating threats to the security of its network is

[19] *See* Petition at 17 that utilize a Wi-Fi hot spot.

legitimate and benefits users of the Wi-Fi network. The Petitioners identify four types of attacks that utilize a Wi-Fi hot spot.[20] However, the security tool they put forward is a blunt instrument that interferes with the operations of authorized devices, including ones that are not a part of the hotels' own networks. Such willful interference against others' authorized uses of unlicensed spectrum is precisely what Section 333 prohibits.

Excluding unlicensed consumer Wi-Fi devices from Section 333's protection, as Petitioners ask the Commission to do here, would not only go against the plain text of the statute, but would also harm consumer welfare and the public interest. A proprietary network operator taking actions in the name of improving its network's reliability or performance could also leverage these actions to compete unfairly and harm consumers. For example, if a customer arrives at a hotel with her own Mi-Fi device and the hotel interferes with the customer's connection to that personal hotspot, the hotel can effectively force the customer to purchase the hotel's Wi-Fi services to gain access, even though the customer has already paid her mobile operator for personal hotspot capability. In effect, the Hotel Industry Interests' proposal would allow entities to use unlicensed spectrum in a proprietary manner, *e.g.*, as if they were operators of licensed spectrum, thereby limiting or preventing access by lawful devices to the unlicensed spectrum, which is a public resource. It is precisely that sort of radiofrequency interference—whether through use of signal jammers or sending signals to de-authenticate rival access points—that Section 333 is designed to prevent.

III. PUBLIC SAFETY CONCERNS

SirenGPS is a company actively developing mobile integrated software solutions for emergency management and public safety. The SirenGPS platform is part of an emerging solution sector

[20] *See* Petition at 7.

that employs WiFi signal as well as cellular data to deliver public safety related information to consumers, emergency managers and to public safety answering points. The availability of wireless data connection as a redundant delivery modality, and in some cases the superior resiliency of wireless internet connection as compared to cellular data connection to mobile devices recommends that the Commission consider the broader picture of the potential impact on public safety of allowing localized restriction on access to wireless internet in public or semi-public places such as hotels and commercial spaces.

The relatively common practice of requiring acceptance of a disclaimer in advance of accessing open wireless internet connection in public spaces through a "splash-page" already poses a threat to public safety by blocking telephone data connections. Many telephone operating systems default to WiFi where a connection is detected, but will be unable to connect to the internet where a splash-page disclaimer limits connection to a local area network until the disclaimer is completed. While we recognize an open WiFi provider's interest in limiting liability for end user activity, this interest is secondary to the value that connected communities, and in turn the Commission, have in advancing public safety. The industry argument that jamming devices are necessary to advance commercial interests for consumers is weak. Market forces will drive hotels to provide the internet connection services that consumers want. We submit that the Commission should consider rule-making and/or recommendation to limit liability to WiFi providers for end user connection and responsibility for end user illicit activity where reasonable care is taken to limit such risk. We strongly urge the Commission to reject any efforts to limit connectivity in public spaces, particularly in hotels, theatres, sports arenas and other places where large numbers of people gather.

IV. CONCLUSION

Section 333 of the Communications Act prohibits willful or malicious interference with a radio-transmitting device authorized under the Communications Act. Unlicensed operations are authorized under the Act, and as a result, are protected under Section 333. The Commission has repeatedly made clear that Wi-Fi is protected from jamming and interference under Section 333, and removing such protection would do harm to consumer welfare and the public interest. For the foregoing reasons, SirenGPS respectfully urges the Commission to deny the Hotel Industry Interests' Petition.

Respectfully submitted,

SIRENGPS, Inc
/s/ Paul Rauner
Paul Rauner
Chief Executive
9272 Olive Street
St Louis, MO 63132
(314) 329-5210
paul.rauner@sirengps.com

Dated: December 25, 2014