

**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 OF HILTON WORLDWIDE HOLDINGS INC. IN SUPPORT OF  
AMERICAN HOTEL & LODGING ASSOCIATION PETITION FOR  
DECLARATORY RULING OR, IN THE ALTERNATIVE, FOR RULEMAKING**

Charles Corbin  
Ama Romaine  
Hilton Worldwide Holdings Inc.  
7930 Jones Branch Drive, 6<sup>th</sup> Floor  
McLean, VA 22102  
(703) 883-5735

*Counsel to Hilton Worldwide Holdings Inc.*

December 19, 2014

**TABLE OF CONTENTS**

I. INTRODUCTION AND SUMMARY ..... 1

II. WI-FI NETWORK OPERATORS HAVE A LEGITIMATE INTEREST  
IN PROVIDING SECURE AND RELIABLE WI-FI SERVICE TO THEIR GUESTS, AND  
REASONABLE MEASURES TO MEET THIS OBJECTIVE ARE CONSISTENT WITH  
SECTION 333 AND PART 15. .... 4

III. CONSTRUING SECTION 333 TO PROHIBIT REASONABLE NETWORK  
MANAGEMENT AND SECURITY MEASURES THAT AFFECT PART 15 DEVICES  
WOULD BE INCONSISTENT WITH THE FEDERAL GOVERNMENT’S  
CYBERSECURITY INITIATIVES AND WOULD EXPOSE WI-FI NETWORK  
OPERATORS TO UNTENABLE LEGAL RISK. .... 11

IV. CONCLUSION ..... 15

**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 OF HILTON WORLDWIDE HOLDINGS INC. IN SUPPORT OF  
AMERICAN HOTEL & LODGING ASSOCIATION PETITION FOR  
DECLARATORY RULING OR, IN THE ALTERNATIVE, FOR RULEMAKING**

**I. INTRODUCTION AND SUMMARY**

Hilton Worldwide Holdings Inc. (“Hilton”) respectfully submits its comments in support of the above-captioned Petition for Declaratory Ruling or, in the Alternative, for Rulemaking (“Petition”) filed by the American Hotel & Lodging Association (“AH&LA”), Marriott International, Inc., and Ryman Hospitality Properties (collectively, “Petitioners”).

Hilton, a member of AH&LA, supports the grant of the relief requested in the Petition, preferably through the issuance of a declaratory ruling or, failing that, through a rulemaking. Hilton submits these separate comments to focus on one particular point: Reasonable network management practices by Wi-Fi operators to protect the reliability and security of those networks for the benefit of their guests should not constitute “willful[] or malicious[] interference” for purposes of Section 333 of the Communications Act, and such practices are therefore permissible under Section 333 and the Commission’s Part 15 rules.

Hilton is one of the largest hospitality companies in the world.<sup>1</sup> For 95 years, it has been committed to providing exceptional guest experiences, and technological innovation is a hallmark of that commitment. For example, Hilton recently announced that its guests will have unprecedented choice and control over their entire hotel stay on their mobile devices, tablets, and computers – including check-in, room choice, and special requests for items to be delivered to their room. And in 2015, Hilton will continue to evolve the guest experience by rolling out mobile-enabled room keys.

Consistent with efforts to meet the needs of its guests, Hilton provides robust, secure broadband Internet connectivity through Wi-Fi networks deployed across its properties. Wi-Fi services are available to overnight guests and, at hotels with meeting and convention facilities, to meeting and convention attendees as well.

Every Wi-Fi network operator has an interest in providing secure and reliable Wi-Fi service, and Hilton is no exception. Hilton goes to great lengths to make sure that a guest or meeting attendee is able to make full use of Hilton's Wi-Fi services without fear of being unable to connect to the Internet due to network congestion or becoming an unsuspecting victim of a cyber-attack.

Providing secure and reliable Wi-Fi service is not easy. For example, Wi-Fi networks are increasingly the target of evolving and sophisticated cyber-attacks. Hilton responds to these threats by employing cutting-edge cybersecurity countermeasures to protect the privacy and data

---

<sup>1</sup> Hilton's portfolio includes more than 4,250 managed, franchised, owned and leased hotels and timeshare properties, comprising over 700,000 rooms in 93 countries and territories. The Hilton brands include Hilton Hotels & Resorts, Waldorf Astoria Hotels & Resorts, Conrad Hotels & Resorts, Curio - A Collection by Hilton, Canopy by Hilton, DoubleTree by Hilton, Embassy Suites Hotels, Hilton Garden Inn, Hampton Hotels, Homewood Suites by Hilton, Home2 Suites by Hilton, and Hilton Grand Vacations.

of its guests and maintain the performance of its Wi-Fi networks. One important tool in this effort is FCC-authorized equipment that is used to manage the Wi-Fi network on hotel premises. Although the capabilities of such equipment vary, they generally include the ability to monitor and mitigate unauthorized access points that pose a threat to the security or reliability of the network. The use of such equipment for these purposes should be encouraged, not prohibited. Indeed, as explained below, guidelines developed by the credit card industry *require* that providers utilize monitoring and mitigation technologies to ensure a safe environment in which to process credit card transactions.

In addition to being unsupported by the text and legislative history of the statute, as explained in the Petition, Hilton is concerned that Section 333, if construed to prohibit Wi-Fi operators from using the capabilities of their FCC-approved Part 15 devices to engage in reasonable network management, could gut a network operator's ability to provide safe and reliable Wi-Fi service.

The statute prohibits a person from "willfully ... interfering with or causing interference to any radio communications of any station licensed by or authorized under this chapter." An overbroad reading of what constitutes "willful[] or malicious[]" interference" could prohibit actions that a Wi-Fi network operator may take to manage its network – no matter how reasonable and laudable and even where such actions use the operator's own Commission-approved Part 15 device in the manner intended – whenever such actions have any effect on another party's Part 15 device. Such an interpretation would undermine the ability of Wi-Fi network operators to use their own Part 15 devices to meet consumer demand for safe and reliable Wi-Fi service at hotels or other establishments, and would be directly contrary to the Commission's objectives in making Part 15 devices widely available and useful to the public.

Such an interpretation would also be inconsistent with the federal government's cybersecurity initiatives, which are dependent upon measures taken by the private sector to protect networks and data, and could expose Wi-Fi network operators to potential liability for any resulting data breach. Indeed, construing Section 333 to prohibit "interference" to a Part 15 device that results from efforts to address a demonstrated threat to an operator's network would run counter to recent Federal Trade Commission ("FTC") and FCC data security efforts.

**II. WI-FI NETWORK OPERATORS HAVE A LEGITIMATE INTEREST IN PROVIDING SECURE AND RELIABLE WI-FI SERVICE TO THEIR GUESTS, AND REASONABLE MEASURES TO MEET THIS OBJECTIVE ARE CONSISTENT WITH SECTION 333 AND PART 15.**

Guests who visit a Hilton hotel reasonably expect that the Wi-Fi service made available on the property will be both safe and reliable. Hilton could not meet its guests' expectations were it unable to manage its Wi-Fi networks, including taking steps to protect against unauthorized access points that pose a threat to the reliability and security of that network.

From a network reliability standpoint, network congestion can be a significant issue. As noted in the Petition (p.4), "Wi-Fi access points are widely available from most electronics stores and ... nearly every smartphone and tablet can function as a Wi-Fi access point." Because these access points operate on a small number of RF channels, in a small meeting space or cramped convention hall multiple guests attempting to operate access points for their own personal benefit (or for the benefit of others) can produce significant interference that renders the airspace almost unusable by anyone seeking to access the Internet via a Wi-Fi connection through the hotel's network. Unless the hotel is allowed to use reasonable network management tools to address this problem, a "tragedy of the commons" ensues such that the common resource of Part 15 spectrum becomes useless to all.

Perhaps in a public space, such as a sidewalk or park, the fact that Part 15 devices create such congestion is simply the luck of the draw, since it is inherent to Part 15 that devices authorized thereunder must accept interference as they find it and do not have interference protection.<sup>2</sup> But there is no reason that a provider cannot take reasonable steps to manage the integrity of its own network on its own private property where such steps do not affect users not on its premises, and the Commission should recognize the legitimacy of such efforts.

Like any other hotel operator, Hilton sometimes needs to address network congestion issues in connection with its offering of Wi-Fi service to guests to assure that those guests have the reliable service they are signing up for. In advocating that reasonable measures to address such congestion be allowed, Hilton is *not* seeking to prevent guests from making any use of personal Wi-Fi access points on hotel property; indeed, Hilton actively encourages such use. Nor would such measures prevent guests from using commonly available non-Wi-Fi technologies for connecting with the Internet, such as a 4G cellular connection using a smartphone, tablet or wireless modem – or from then connecting additional devices to such a primary connection using non-Wi-Fi means, such as an Ethernet cable or Bluetooth connection.<sup>3</sup> In short, Hilton is not seeking to use reasonable network management techniques as a pretext to compel guests to purchase Wi-Fi services from Hilton when visiting one of its hotels.

---

<sup>2</sup> See *Revision of Part 15 of the Rules regarding the operation of radio frequency devices without an individual license, First Report and Order (“Part 15 Revision Order”)*, 4 FCC Rcd 3493, 3507, 3514-15 (1989); 47 CFR §§ 15.5(b), 15.19(a)(3).

<sup>3</sup> To be sure, the interior of a conference center made of concrete and steel may lack the cellular signal strength needed to obtain a usable 4G signal. While there is no legal obligation for Hilton to overcome this problem, the market dictates otherwise – Hilton guests expect their 4G devices to get a usable signal, and Hilton has a strong incentive to respond to this expectation. For this reason, Hilton has expended – and is continuing to expend – substantial efforts and money working with mobile carriers to install DAS systems and related technical solutions to improve cellular reception within its owned and managed properties.

Allowing Hilton and other Wi-Fi operators to take reasonable steps to assure network reliability is not inimical to Commission policies or the objectives of the Communications Act. To the contrary, in a different context the Commission has recognized that reasonable network management is *critical* if consumers are to enjoy the benefits of a flourishing and open Internet.<sup>4</sup> According to the Commission, a network management practice is reasonable “if it is appropriate and tailored to achieving a legitimate network management purpose,” which includes “ensuring network security and integrity, including by addressing traffic that is harmful to the network; addressing traffic that is unwanted by end users (including by premise operators), such as by providing services or capabilities consistent with an end user’s choices regarding parental controls or security capabilities; and reducing or mitigating the effects of congestion on the network.”<sup>5</sup>

Importantly, the ability of a broadband provider to take steps to address network congestion is not limited to licensed spectrum: the Commission has specifically recognized the importance of reasonable network management in the unlicensed spectrum context, which poses “unique network management challenges,” because such “spectrum is shared among multiple users and technologies and no single user can control or assure access to the spectrum.”<sup>6</sup> Having recognized that appropriate network management measures are not only legitimate but important to further vital policy objectives, it would be folly for the Commission now to prohibit the same measures as “interference” under Section 333.

---

<sup>4</sup> *Preserving the Open Internet; Broadband Industry Practices*, Report and Order, 25 FCC Rcd 17905, ¶ 80 (2010) (“*Open Internet Order*”), *aff’d in part, vacated and remanded in part sub nom. Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

<sup>5</sup> *Open Internet Order* ¶ 82 (footnotes omitted); *see also id.* ¶ 91 (recognizing that “congestion management may be a legitimate network management purpose”).

<sup>6</sup> *Id.* ¶ 86.



Nor is the *Open Internet Order* an outlier in this regard. On a number of other occasions, even with regard to *licensed* services, the Commission has expressly recognized the distinction between reasonable network management, on the one hand, and “interference” prohibited by Section 333, on the other. For example, in its *Contraband Wireless Device Order*, the Commission sought to address the steps authorities might take to stem the unauthorized use of cell phones inside correctional facilities.<sup>7</sup> The Commission observed that “[t]echnological solutions available to correctional facility administrators to combat contraband wireless devices generally fall into three categories: managed access, detection, and radio signal jamming.”<sup>8</sup> Managed access systems, which the Commission noted were already permitted when authorized by the Commission, were described as follows:

Managed access systems are micro-cellular, private networks that analyze transmissions to and from wireless devices to determine whether the device is authorized or unauthorized for purposes of accessing public carrier networks. Managed access systems utilize base stations that are optimized to capture all voice, text, and data communications within the system coverage area, which would be a correctional facility in the instant case. When a wireless device attempts to connect to the network from within the coverage area of the managed access system, the system cross-checks the identifying information of the device against a database that lists wireless devices authorized to operate in the coverage area. *Authorized devices are allowed to communicate normally (i.e., transmit and receive voice, text, and data) with the commercial wireless network, while transmissions to or from unauthorized devices are terminated.* The managed access system may also provide an alert to the user notifying the user that the device is unauthorized. The systems provide operational flexibility to the correctional facility administrators by allowing them to disable devices without having to physically remove them.<sup>9</sup>

---

<sup>7</sup> *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Notice of Proposed Rulemaking, FCC 13-58, 28 FCC Rcd 6603 (2013) (“*Contraband Wireless Device Order*”).

<sup>8</sup> *Id.* ¶ 13.

<sup>9</sup> *Id.* ¶ 14 (emphasis added, citations omitted).

The Commission expressly contrasted this technique with the use of jammers. Although some parties argued that correctional authorities should be permitted to use jammers, the Commission flatly rejected this idea, pointing out that “[t]he Act prohibits any person from willfully or maliciously interfering with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government. Because radio signal jammers are used to willfully interfere with radio communications of such licensed or authorized stations, jammers are not permitted under the Commission’s rules.”<sup>10</sup> Nowhere in the Commission’s discussion is there any hint that managed access systems would result in prohibited “interference,” and it is clear that the Commission did not believe that the scope of the Section 333 prohibition extends to network management.<sup>11</sup>

From a security standpoint, attacks on privately-operated computer networks are increasing in number and sophistication.<sup>12</sup> Hotel networks are no exception to this trend; those with meeting and convention facilities are an especially attractive target for cyber criminals seeking to purloin credit card or other personally identifiable information from guests.<sup>13</sup>

---

<sup>10</sup> *Id.* ¶ 19.

<sup>11</sup> The Commission drew a similar distinction in *Expanding Access to Mobile Wireless Servs. Onboard Aircraft*, Notice of Proposed Rulemaking, 28 FCC Rcd 17132, ¶ 62 (2013), tentatively concluding that the functionality under consideration there “constitutes a proper network management function and is not the willful or malicious interference at issue in Section 333.”

<sup>12</sup> See U.S. Gov’t Accountability Office, GAO-13-187, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented* 3–12 (2013).

<sup>13</sup> See, e.g., Mike Freeman, “Cyber Attack Hits San Diego Hotel Chain,” *The San Diego Union-Tribune* (Sept. 9, 2014), <http://www.utsandiego.com/news/2014/sep/09/target-home-depot-bartell-hotels-cyber-hacking/>; Andy Greenberg, “Cybercrime Checks Into Hotels,” *Forbes* (Feb. 2, 2010) (noting that “America’s hotels have had some uninvited guests: a wave of increasingly sophisticated invasions by organized cybercriminals”),

Hotel Wi-Fi networks, in particular, are a tempting point of attack because their inherent characteristics make them harder to secure and protect than traditional wired networks. As the Petitioners demonstrate, Wi-Fi networks can be used to launch a variety of attacks against guests, including threats from signal interception, unauthorized network access, unauthorized access points, and access point spoofing.<sup>14</sup>

The security threats faced by hotels are neither speculative nor hypothetical. For example, Kaspersky Labs recently reported an advanced, persistent threat known as the “Darkhotel APT” that targets individual hotel guests attempting to connect to the Internet over a hotel’s Wi-Fi network.<sup>15</sup> The Darkhotel APT utilizes sophisticated tools and techniques including zero day exploits, forged certificates, and enhanced keyloggers to gain access to the target’s computer system.<sup>16</sup> Kaspersky reports that targets tend to be high-profile guests such as top-level executives of large companies.<sup>17</sup> Other experts have suggested that members of the U.S. defense industrial base are also being targeted.<sup>18</sup> And the Darkhotel APT is not only the threat: several years ago, the FBI warned of similar efforts to target guests attempting to connect

---

*footnote cont’d.*

<http://www.forbes.com/2010/02/01/cybersecurity-breaches-trustwave-technology-security-hotels.html>.

<sup>14</sup> See Petition, at 8-12.

<sup>15</sup> See Kaspersky Labs, *The Darkhotel APT: A Story of Unusual Hospitality* 3 (Nov. 2014).

<sup>16</sup> See *id.*

<sup>17</sup> See *id.* at 27.

<sup>18</sup> See, e.g., Kim Zetter, *DarkHotel: A Sophisticated New Hacking Attack Targets High-Profile Hotel Guests*, *Wired* (Nov. 10, 2014), <http://www.wired.com/2014/11/darkhotel-malware/>.

to Wi-Fi networks from their hotel rooms.<sup>19</sup> Hotels must be allowed to use the tools available to them to detect and shut down these attacks on their guests.

A hotel operating a Wi-Fi network also must take special security precautions given the volume of credit card transactions it processes. Like many other businesses, Hilton is required to comply with the Payment Card Industry (PCI) Data Security Standard (DSS), which was developed to encourage and enhance cardholder data security and facilitate the global adoption of consistent data security measures.<sup>20</sup> The PCI DSS, which provides a baseline of technical and operational requirements designed to protect data of credit card holders, applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. Of particular relevance to this proceeding, the PCI DSS requires that covered entities “test for the presence of wireless access points and detect unauthorized wireless access points.” As part of the testing procedure, a covered entity is required to put in place an “incident response plan” that “includes a response in the event unauthorized wireless devices are detected.”<sup>21</sup>

Hilton agrees with Petitioners that if a hotel is powerless to address activities that threaten “the security and reliability of its Wi-Fi network on its premises, both the hotel and guests would suffer.”<sup>22</sup> The Commission must ensure that hotel operators are able to protect themselves, their

---

<sup>19</sup> See Internet Crime Complaint Center (IC3), *Public Service Announcement: Malware Installed on Traveler’s Laptops Through Software Updates on Hotel Internet Connections* (May 8, 2012), available at <http://www.ic3.gov/media/2012/120508.aspx>.

<sup>20</sup> PCI Security Standards Council LLC, *PCI DSS Requirements and Security Assessment Procedures*, Version 2.0, at 5 (Oct. 2010).

<sup>21</sup> *Id.* at 59-69, §§ 11.1, 12.9.

<sup>22</sup> Petition, at 4.

guests, and their networks from threats to network reliability and security posed by other wireless access points being used on their premises.

### **III. CONSTRUING SECTION 333 TO PROHIBIT REASONABLE NETWORK MANAGEMENT AND SECURITY MEASURES THAT AFFECT PART 15 DEVICES WOULD BE INCONSISTENT WITH THE FEDERAL GOVERNMENT’S CYBERSECURITY INITIATIVES AND WOULD EXPOSE WI-FI NETWORK OPERATORS TO UNTENABLE LEGAL RISK.**

The federal government’s focus on cybersecurity and data security underscores the need for a Wi-Fi operator to be able to detect and mitigate unauthorized access points that may pose a threat to its network or guests. President Obama made cybersecurity a priority with the release of Executive Order 13636, Improving Critical Infrastructure Cybersecurity (the “Executive Order”).<sup>23</sup> The Executive Order stressed that “[r]epeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity” and that “[t]he national and economic security of the United States depends on the reliable functioning of the Nation’s critical infrastructure in the face of such threats.”<sup>24</sup> It champions public-private collaboration “to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”<sup>25</sup>

Federal agencies routinely engage the private sector on cyber and data security. For example, the President’s National Security Telecommunications Advisory Committee (“NSTAC”) convenes industry leaders to advise the U.S. Government on security issues relating to telecommunications services. At a recent NSTAC meeting, Chairman Wheeler stated that “the solutions to counter aggressive, thinking adversaries ... come from the front lines—from the

---

<sup>23</sup> See Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) (“Improving Critical Infrastructure Cybersecurity”).

<sup>24</sup> *Id.*, § 1.

<sup>25</sup> *Id.*

network operators and service providers who are under attack every day.”<sup>26</sup> Similarly, the FCC’s Communications Security, Reliability and Interoperability Council (“CSRIC”), which includes industry leaders, provides recommendations to the Commission concerning issues relating to the security of various communications systems. These platforms allow industry to lend their expertise to the government, and provide policymakers with an opportunity to encourage industry efforts that further the government’s cybersecurity initiatives.

In addition to encouraging private industry to become more engaged in cybersecurity efforts, federal agencies have sought to achieve similar engagement by initiating enforcement actions for data security lapses. The FTC recently brought suit against a hotel chain for alleged failures to protect adequately the personal information of its guests in violation of Section 5 of the FTC Act – a suit that a federal district court held the FTC had the jurisdiction to bring.<sup>27</sup> In *FTC v. Wyndham Worldwide Corp.*, the FTC alleges that the hotel chain’s “information security failures led to the compromise of many of the [hotels’] property management system servers, resulting in the exposure of thousands of consumers’ payment card accounts” and amounting to an “unfair and deceptive business practice.”<sup>28</sup> According to the FTC’s complaint, the hotel “unreasonably and unnecessarily exposed consumers’ personal data to unauthorized access and theft,” “failed to employ reasonable measures to detect and prevent unauthorized access to [its]

---

<sup>26</sup> See NSTAC Closed Session, *Remarks of Chairman Tom Wheeler* (Nov. 19, 2014), available at <http://www.fcc.gov/document/remarks-chairman-tom-wheeler-nstac-closed-session>.

<sup>27</sup> See *F.T.C. v. Wyndham Worldwide Corp.*, 10 F.Supp.3d 602 (D.N.J. Apr. 7, 2014).

<sup>28</sup> Complaint of the Federal Trade Commission, *F.T.C. v. Wyndham Worldwide Corp.*, No. CIV.A. 13-1887 (June 26, 2012).

computer network or to conduct security investigations,” and “failed to use readily available security measures.”<sup>29</sup>

Similarly, the FCC recently released a Notice of Apparent Liability (“NAL”) proposing a \$10 million forfeiture against two carriers for violations of the Communications Act stemming from allegedly inadequate data security practices.<sup>30</sup> The NAL charges that “[b]y failing to employ reasonable data security practices to protect consumers’ [proprietary information], the Companies . . . engaged in an unjust and unreasonable practice in apparent violation of Section 201(b) of the [Communications] Act. They failed to use even the most basic and readily available technologies and security features and thus created an unreasonable risk of unauthorized access.”<sup>31</sup>

In light of these actions, it would be beyond ironic for the Commission to endorse an interpretation of Section 333 that prevents a Wi-Fi operator from managing its network to ensure secure and reliable service. On the one hand, failure to implement adequate data security measures that mitigate the threat of an unauthorized access point may expose a Wi-Fi operator to an enforcement action for a failure to “employ reasonable measures to detect and prevent unauthorized access.” But, on the other hand, unless the Commission makes clear that Section 333 does not forbid reasonable network management measures, taking such measures to protect data security may result in an enforcement action under Section 333 when they cause “interference” to a Part 15 device.

---

<sup>29</sup> *Id.*, at ¶ 24.

<sup>30</sup> *See Terracom, Inc. & Yourtel Am., Inc.*, Notice of Apparent Liability for Forfeiture, FCC 14-173 (Oct. 24, 2014).

<sup>31</sup> *Id.*, ¶ 12.

Wi-Fi operators faced with this regulatory Hobson’s choice could hardly be blamed for taking the path of least resistance, implementing only the security measures that are explicitly endorsed or required by the government and hoping that at least these will survive Section 333 scrutiny. But according to Chairman Wheeler, the FCC expects private entities to “step up” and proactively manage risks posed by cyber threats.<sup>32</sup> Tying a Wi-Fi operator’s hands by construing Section 333 to ban efforts to mitigate threats to network security and reliability would have the opposite effect. And forcing operators to navigate the impossibly narrow compliance channel implicit in this choice would be exactly the “check-the-block list of compliance” mentality that Chairman Wheeler expressly rejected as inadequate to counter “threats [that] move faster than a notice-and-comment rulemaking process.”<sup>33</sup>

---

<sup>32</sup> See NSTAC Closed Session, *Remarks of Chairman Tom Wheeler* (Nov. 19, 2014), available at <http://www.fcc.gov/document/remarks-chairman-tom-wheeler-nstac-closed-session>.


<sup>33</sup> See *id.* See also *President’s Remarks on Securing the Nation’s Information and Communications Infrastructure*, 1 Pub. Papers 731, 734 (May 29, 2009) (“[L]et me be very clear: My administration will not dictate security standards for private companies.”).



#### IV. CONCLUSION

For the foregoing reasons, the Commission should grant the Petition and find that Section 333 does not preclude reasonable network management measures that affect Part 15 devices on the premises of the network operator. At the very least, the Commission should clarify the circumstances under which “interference” to a Part 15 device that is the result of a Wi-Fi operator’s use of FCC-authorized equipment to protect the reliability and security of its network for the benefit of its guests is permissible under Section 333 and the Commission’s Part 15 rules.

Respectfully submitted,

By:  \_\_\_\_\_

Charles Corbin  
Ama Romaine  
Hilton Worldwide Holdings Inc.  
7930 Jones Branch Drive, 6<sup>th</sup> Floor  
McLean, VA 22102  
(703) 883-5735

*Counsel to Hilton Worldwide Holdings Inc.*

December 19, 2014

