

RM-11737

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 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

ACCEPTED/FILED

AUG 25 2014

Docket No. _____

Federal Communications Commission
Office of the Secretary

PETITION FOR DECLARATORY RULING OR, IN THE
ALTERNATIVE, FOR RULEMAKING

Banks Brown
McDermott Will & Emery LLP
340 Madison Avenue
New York, NY 10173-1922
212 547 5488

*Counsel for the American
Hospitality & Lodging Association*

Bennett L. Ross
David Hilliard
Henry Gola
Wiley Rein LLP
1750 K Street, NW
Washington, DC 20006
(202) 719-7000

*Counsel for Marriott International, Inc. and
Ryman Hospitality Properties*

August 25, 2014

WTB 14-27

TABLE OF CONTENTS

	<u>PAGE</u>
I. INTRODUCTION AND SUMMARY	2
II. STATEMENT OF THE FACTS	6
A. Wi-Fi Operators Should Have The Ability to Manage Their Networks In Order To Offer Secure And Reliable Wi-Fi Service.	6
B. Wi-Fi Operators Manage Their Networks By Using Equipment Authorized By The FCC That Monitors And Mitigates Security Threats And Network Interference.	8
III. ARGUMENT.....	13
A. The Commission Should Clarify That A Wi-Fi Network Operator's Management Of Its Network That May Cause "Interference" To A Part 15 Device Used By A Guest On the Operator's Property Does Not Violate Section 333.	13
B. In The Alternative, The Commission Should Initiate A Rulemaking To Amend Its Part 15 Rules To Specify The Interference To Part 15 Devices That Section 333 Prohibits.	19
IV. CONCLUSION	22

¹ 47 C.F.R. § 1.2; 47 C.F.R. § 1.401.

I. INTRODUCTION AND SUMMARY

Wi-Fi has become the method of choice for connecting to the Internet.² Most airports, government offices (including the FCC), educational institutions, as well as many commercial establishments operate Wi-Fi networks to meet user demand. Within the hospitality sector, hotels have deployed Wi-Fi networks to provide Internet connectivity to their guests and meeting and convention attendees.

Serving the hospitality industry for more than a century, the AH&LA is the sole national association representing all segments of the 1.8 million-employee U.S. lodging industry, including hotel owners, REITs, chains, franchisees, management companies, independent properties, state hotel associations, and industry suppliers. Headquartered in Washington, D.C., AH&LA provides focused advocacy, communications support, and educational resources for an industry generating \$155.5 billion in annual sales from 4.9 million guestrooms.

Marriott is a leading hospitality company founded by J. Willard and Alice S. Marriott in 1927 and guided by J.W. "Bill" Marriott, Jr. for nearly 60 years. Headquartered in Bethesda, Maryland, Marriott and its hotels employ approximately 325,000 associates worldwide and operate more than 4,000 properties across 18 lodging brands in more than 70 countries and territories around the world.

Ryman is a real estate investment trust specializing in group-oriented, destination hotel assets in urban and resort markets. Its managed assets include a network of four upscale, meetings-focused resorts totaling 7,795 rooms managed by Marriott under the Gaylord Hotels brand – the Gaylord Opryland Resort, the Gaylord Texan Resort, the Gaylord National Resort, and the Gaylord Palms Resort.

² The term Wi-Fi (Wireless-Fidelity) refers to unlicensed wireless devices operating in the 2.4 GHz and 5 GHz regions of the spectrum in accordance with the Institute of Electrical and Electronics Engineers ("IEEE") 802.11 standards.

In this Petition, AH&LA, Marriott, and Ryman seek to clarify the extent to which a Wi-Fi operator can manage its network without running afoul of 47 U.S.C. § 333, which provides 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.” Specifically, 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, even when doing so may result in “interference” to a Part 15 device being operated by a guest on its property.

At the outset, it is important to point out what this Petition is not about. First, this Petition does not involve any actual or threatened interference to licensed spectrum or spectrum used by the government. Such interference is plainly prohibited by Section 333.

Second, this Petition does not implicate the Commission’s “network neutrality” rules. Those rules do not apply to “premise operators,” which include establishments “such as coffee shops, bookstores, airlines, and other entities when they acquire Internet service from a broadband provider to enable their patrons to access the Internet from their establishments.”³

Third, the Petition does not involve signal jammers, which transmit “powerful radio signals that overpower, jam, or interfere with authorized communications.”⁴ According to the

³ See *Preserving the Open Internet*, Report and Order, 25 FCC Rcd 17905, ¶ 52 (2010); see also *id.* ¶ 45 (applying rules to “broadband Internet access service,” which is defined as a “mass market” service “marketed and sold on a standardized basis to residential customers, small businesses, and other end-user customers such as schools and libraries”); 47 C.F.R. § 8.11(a).

⁴ *C.T.S. Technology Co., Limited*, Notice of Apparent Liability for Forfeiture and Order, FCC 14-92, ¶ 2 (rel. June 19, 2014) (“*CTS Notice of Apparent Liability*”); see also *Office of Engineering and Technology and Compliance and Information Bureau Warn Against the Manufacture, Importation, Marketing or Operation of Transmitters Designed to Prevent or Otherwise Interfere with Cellular Radio Communications*, DA 99-2150 (rel. October 12, 1999).

FCC, signal jammers “have no lawful consumer use in the United States,”⁵ which is in stark contrast to the network management equipment that is the subject of this Petition, which Petitioners understand the Commission has authorized for use in the United States.

As Wi-Fi becomes increasingly popular for connecting to the Internet, it is imperative that the Commission clarify the rules of the road for Wi-Fi network operators. As explained below, Wi-Fi network operators should be able to manage their networks in order to provide a secure and reliable Wi-Fi service to guests on their premises. This is particularly true when Wi-Fi access points are widely available from most electronics stores and when nearly every smartphone and tablet can function as a Wi-Fi access point. In addition, some vendors offer platforms designed for high-density environments that include access points capable of supporting thousands of simultaneous Wi-Fi users.

Any access point can be used to launch an attack against an operator’s network or threaten its guests’ privacy (for example, by attempting to obtain guests’ credit card or other personal information). Likewise, multiple Wi-Fi access points operating in a meeting room or on a convention floor of a hotel can adversely affect the performance of the hotel’s Wi-Fi network. If a hotel is powerless to address such activities to ensure the security and reliability of its Wi-Fi network on its premises, both the hotel and its guests would suffer.

Section 333 was enacted in 1990 to prohibit interference to licensed radio communications services as well as those services operating without an individual station license, such as citizens band radio services. Section 333 was not intended – and the FCC has never interpreted the statute – to prohibit interference to a Wi-Fi access point or any Part 15

⁵ *CTS Notice of Apparent Liability* ¶ 2. In limited circumstances and consistent with applicable procurement requirements, jamming devices may be marketed to the federal government for authorized, official use. See 47 U.S.C. § 302a(c); 47 C.F.R. § 2.807(d).

device. Indeed, extending Section 333 to prohibit interference to Part 15 devices would be legally unsustainable. By the statute's plain terms, Section 333 only safeguards stations "licensed or authorized by or under this chapter." Part 15 devices are not "licensed" nor were they specifically "authorized by or under" the Communications Act at the time Section 333 was enacted. Furthermore, the statute's legislative history confirms that Congress did not intend Section 333 to apply to interference to Part 15 devices, even though the Commission's Part 15 rules had been in place long before Congress enacted Section 333.

Interpreting Section 333 to prohibit interference to Part 15 devices also would be inconsistent with the Commission's Part 15 rules. As the Commission has made clear, interference to a Part 15 device does not constitute "harmful interference," which is the only interference Part 15 prohibits. An interpretation of Section 333 to prohibit interference to a Part 15 device when such interference is not prohibited by the Part 15 rules under which the device is authorized to operate would be legally infirm. It also would lead to absurd results by making interference to any Part 15 devices – such as cordless telephones, baby monitors, and garage door openers – a violation of federal law.

Even assuming Section 333 governs interference to Part 15 devices (which is not the case), the Commission should clarify that a Wi-Fi network operator does not violate Section 333 when any interference results from the use of FCC-authorized equipment in managing its network and affects Part 15 devices used by guests on the operator's property. Because the equipment authorization process requires a demonstration that the Part 15 device complies with the Commission's rules, a Wi-Fi network operator should not lawfully be subject to sanction when using that equipment in the manner intended. Furthermore, extending Section 333 to Part 15 devices would be inconsistent with the Commission's Over-the-Air Reception Devices

(“OTARD”) rules by giving guests superior rights as compared to owners or lessors of property in their use of Part 15 devices.

In the alternative, the Commission should initiate a rulemaking to modify its Part 15 rules to specify the interference to Part 15 devices that Section 333 prohibits. The Commission’s Part 15 rules cannot be reconciled with Section 333, since the former currently do not prohibit interference to Part 15 devices. The Commission can only address this anomaly through a notice and comment rulemaking. Furthermore, issues surrounding whether and to what extent a Wi-Fi network operator can monitor and mitigate interference by Part 15 devices – for example, to stop a potential data security breach – affect operators, equipment manufacturers, and consumers alike. Because these issues substantively impact the public to a sufficient degree, the Commission should address these issues in a rulemaking.

II. STATEMENT OF THE FACTS

A. Wi-Fi Operators Should Have The Ability to Manage Their Networks In Order To Offer Secure And Reliable Wi-Fi Service.

Hotels large and small provide wireless Wi-Fi services. As a matter of convenience and competitive necessity, hotels routinely make available Wi-Fi service to their guests as a means to connect to the Internet and access information and services related to their stay. For those hotels offering meeting or convention facilities, they often provide Wi-Fi and other Internet connectivity services to meeting planners, meeting attendees, exhibitors, and their customers. Like other Wi-Fi operators, hotels utilize 2.4 GHz and 5 GHz frequency in providing Wi-Fi service.

When a customer elects to purchase Wi-Fi service in connection with a meeting or convention, a hotel often will commit to the technical parameters of the service it will provide and the price it will charge. Hotels take seriously their obligation to provide meeting planners,

meeting attendees, exhibitors, and their customers who elect to purchase Wi-Fi services with the quality of service they expect and to which they are entitled.

Because it utilizes radio frequency ("RF"), a Wi-Fi network presents numerous operational challenges and is inherently difficult to control and protect. For example, Wi-Fi networks are more susceptible to a variety of attacks that can threaten the security and reliability of a hotel's network or pose a risk to guests, including: (i) signal interception; (ii) unauthorized network access; (iii) unauthorized access points; and (iv) access point spoofing. Individuals can utilize a Wi-Fi hot spot in order to execute any of these various attacks.

To illustrate, in an access point spoofing (or "honey pot") attack, an intruder sets up an access point (which can be purchased at almost any electronics store) in a hotel meeting room or convention center and begins advertising the service set identifier ("SSID") of the hotel's Wi-Fi network. Unsuspecting guest devices associate to the intruder's access point, believing they are roaming through a valid access point. The intruder then gets direct access to guest devices, enabling a number of additional attacks such as man-in-the-middle, Address Resolution Protocol poisoning, DHCP/DNS hijacking, and injection of network worms and viruses.⁶

Even users not intending to engage in malicious conduct nonetheless can threaten the reliability of a hotel's Wi-Fi network by establishing unauthorized access points, particularly in meeting spaces and convention facilities. With more and more Wi-Fi-enabled devices utilizing hotel networks, and as users increasingly demand more reliable Wi-Fi connections capable of supporting streaming multimedia applications, unauthorized access points can hinder the ability

⁶ One such virus is a so-called "Trojan Horse," which appears to be performing a desirable task for the user when in reality the virus permits the intruder to access remotely the user's device. With such access, the intruder can steal the user's data, such as credit card information or passwords, upload or download files, or utilize the device for a botnet attack, for spamming, or launching denial of service attacks.

of meeting or convention attendees to access the hotel's Wi-Fi network or reduce its throughput. Without the ability to address RF interference, hotel guests would almost invariably experience unreliable Wi-Fi performance, spotty coverage, and dropped connections. Customers who encounter a negative Wi-Fi experience often blame the hotel, thus potentially damaging the hotel's reputation. It also may cause meeting or convention planners to seek refunds or in some cases monetary compensation from a hotel that has failed to deliver the Wi-Fi service it promised.

B. Wi-Fi Operators Manage Their Networks By Using Equipment Authorized By The FCC That Monitors And Mitigates Security Threats And Network Interference.

In order to protect their guests and provide a Wi-Fi signal that delivers the best possible throughput, many hotels take steps to monitor and mitigate RF interference, which can be generated by almost any device that emits an electro-magnetic signal. In particular, hotels have purchased and installed network management systems manufactured by a host of vendors – including Aruba Networks and Cisco, among others – that allow a hotel to manage its Wi-Fi networks. As far as Petitioners are aware, the FCC has authorized these types of network management equipment pursuant to its equipment authorization rules.⁷

Although the functionality of these network management systems varies, they typically provide visibility into activities affecting the quality of wireless Internet connectivity provided by a Wi-Fi network operator, including Wi-Fi coverage and access points.⁸ For example,

⁷ See 47 C.F.R. §§ 2.803, 2.901, 15.201(b).

⁸ See <http://www.airtightnetworks.com/home/solutions/wireless-intrusion-prevention.html> (AirTight's Wireless Intrusion Prevention System "is consistently recognized as the industry's top rated wireless IPS solution and is the solution of choice for security conscious organizations across all markets including retail, financial services, healthcare, Federal government and DoD installations"); <http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-Enterprise> (offering systems "with integrated spectrum and 802.11n analysis for complete

network management equipment manufactured and made available for sale in the U.S. by Aruba Networks allows a Wi-Fi network operator to identify what types of devices are on its network, where the devices are accessing the network, and the bandwidth they consume. The Aruba Networks platform also uses wireless access points to scan the RF environment for unauthorized devices that are interfering or potentially could interfere with the Wi-Fi operator's network.⁹

Various network management systems offered for sale in the U.S. also include the capability to mitigate access points that pose a threat to a Wi-Fi operator's network or could adversely affect the Wi-Fi service provided to customers.¹⁰ This capability can include both automated and manual mitigation functionalities. For example, the Aruba Networks platform can be configured to identify and contain unauthorized access points. For a device attempting to connect to an unauthorized access point, the Aruba Networks platform will send de-authentication packets which prevent that connection from being completed.¹¹

(footnote cont'd.)

visibility and control"); <http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html> (offering "a number of methods to detect Wi-Fi-based rogue devices including off-channel scanning and dedicated monitor mode capabilities").

⁹ Additional information regarding the Aruba Networks platform is available at <http://www.arubanetworks.com>.

¹⁰ See, e.g., <http://www.airtightnetworks.com/home/products/airtight-wips.html> (describing Airtight's system that can "block Wi-Fi network access to unapproved devices"); <http://www.flukenetworks.com/content/datasheet-airmagnet-enterprise> (offering the industry's most thorough wireless monitoring with leading research, analysis and threat remediation"); <http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html> (describing "rogue mitigation" capabilities to contain "rogue Access Points (APs), wireless router, rogue clients, and rogue ad-hoc networks").

¹¹ This Petition does not address attempts to mitigate operations occurring outside the premises of a Wi-Fi network operator. Equipment can now pinpoint the location of unauthorized access points and avoid attempting to mitigate the effect of any access points located off the operator's property, such as at a neighboring business or residence. Thus, this Petition does not seek to have the Commission find that Wi-Fi network operators should have the ability to address the use of Part 15 devices occurring off the operator's premises.

These network management systems are not just used by hotels. Rather, Petitioners understand that such systems are routinely sold to and regularly used by other operators of Wi-Fi networks, including the federal government, state and local governments, enterprise customers, and educational institutions.¹²

For example, many large universities operating networks that include Wi-Fi employ various techniques to ensure network performance. Duke University, for example, limits students to “a daily threshold of 5 GB” on Duke’s network; students who repeatedly exceed this threshold will have “the outbound bandwidth” of their computers “restricted to 64 kb/s (kilobits per second) for the remainder of the semester.”¹³ Georgetown University prohibits students from using network resources to illegally share music or to consume excessive amounts of storage and “reserves the right to limit access to its networks through University-owned or other computers”¹⁴ Likewise, according to Northwestern University, in order to protect its network from “a network-intensive application or a defective computer,” the University will “disconnect[] the offending computer system from the network until the problem is resolved. If the condition is an imminent hazard to the University network or disrupts the activities of others, then the offending

¹² Aruba Networks recently announced that the Prince George’s County Public Schools (“PGCPS”) district in Maryland is deploying an Aruba Mobility-Defined Network in its 204 schools and 20 other school system facilities. According to Aruba, PGCPS has experienced an influx of mobile device use at its facilities, which will require the deployment of more than 15,000 access points in its facilities as part of the network upgrade. http://www.businesswire.com/news/home/20140805005103/en#U-IQQtfd_X6.

¹³ Duke Office of Information Technology, ResNet bandwidth constraints: Addressing bandwidth utilization, at <http://oit.duke.edu/net-security/network/resnet-policy.php> (last visited Aug. 14, 2014).

¹⁴ Georgetown University Information Security Office, Acceptable Use Policy, at <http://security.georgetown.edu/technology-policies/acceptable-use> (last visited Aug. 14, 2014).

computer system or the subnet to which it is attached may be disconnected without prior notice.”¹⁵

Petitioners’ purpose is not to single out prominent universities for Commission scrutiny. Rather, the point is simply that the network management policies of these educational institutions underscore that Wi-Fi network operators – regardless of the businesses in which they are engaged or the constituencies they serve – must manage actively their networks. A critical component of such network management is the use of equipment authorized by the FCC that protects the security and integrity of the Wi-Fi services being provided.

The increased availability of Wi-Fi – particularly mobile hot spots – has put a premium on the need for equipment to monitor and, if necessary, mitigate unauthorized access points that threaten the security and reliability of an operator’s Wi-Fi network. According to Cisco’s 2014 Visual Networking Index (“VNI”), the increased proliferation of Wi-Fi hotspots will lead to more data traffic being delivered via Wi-Fi networks than wired networks by 2018.¹⁶ The VNI predicts that by 2018, Wi-Fi will generate 49 percent of all of IP traffic, as compared to 39 percent for fixed line traffic and 12 percent for cellular.¹⁷

In today’s marketplace, nearly every smartphone and tablet – of which, according to CTIA, there are approximately 200 million in use in the U.S. today – can serve as a Wi-Fi hotspot. In addition, some vendors offer a high-radio density Wi-Fi platform to meeting and

¹⁵ Northwestern University Information Technology, Use of Student Residence Networks, at <http://www.it.northwestern.edu/policies/resnet.html> (last visited Aug. 14, 2014). Attached as Appendix 1 is an overview of the network management practices of more than 20 large and prestigious universities in the United States.

¹⁶ Sue Marek, *Cisco Study: 79% of All IP Traffic Will be Video by 2018*, FierceCable.com (June 9, 2014), available at <http://www.fiercecable.com/story/cisco-study-79-all-ip-traffic-will-be-video-2018/2014-06-09>.

¹⁷ *Id.*

convention planners that features hot spots capable of supporting multiple devices.¹⁸ A single hotspot created by a guest using his or her smartphone or tablet can cause security or interference issues by, for example, adding another SSID into the air, which can confuse other devices attempting to connect to the Internet. Multiple hot spots, especially when located in close proximity to one another, can create an almost unusable airspace that hinders Wi-Fi service. With multiple hot spots operating in a meeting room or on a convention floor, unless the transmit signal power of each device is reduced, the access points generate interference to each other, a phenomenon known as co-channel interference.

One approach to dealing with Wi-Fi interference is “channel changing,” which occurs when a different or “cleaner” channel is automatically selected for the access point when RF interference increases. However, within the 2.4 GHz frequency, the most widely used Wi-Fi band, there are only three non-interfering channels. Even within the 5 GHz band, only four non-overlapping 40MHz wide channels currently exist. With limited channels to which to change in an effort to deal with Wi-Fi interference, the changing of channel assignments can cause problems for other users because it requires connected clients to disassociate and re-associate, causing disruption to voice and video applications and creating a domino effect as neighboring access points change channels to avoid co-channel interference.¹⁹

¹⁸ See <http://www.xirrus.com/Products/Wireless-Arrays> (“The industry’s only multi-radio Wi-Fi platform, supporting 2 to 16 radios, Xirrus modular Arrays include an integrated controller and multi-core processing to scale up to very large densities of mobile users”).

¹⁹ To its credit, the Commission is taking steps to address Wi-Fi congestion by freeing up 100 MHz in the 5GHz band for unlicensed use. *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, First Report and Order, 29 FCC Rcd 4127 (2014) (“5 GHz Order”). And, while this decision provides “much-needed relief to the growing problem of congestion on Wi-Fi networks,” *id.*, Statement of Chairman Tom Wheeler, the availability of additional Wi-Fi capacity will not eliminate the need for Wi-Fi operators to manage their networks to ensure they provide secure and reliable service.

III. ARGUMENT

A. The Commission Should Clarify That A Wi-Fi Network Operator's Management Of Its Network That May Cause "Interference" To A Part 15 Device Used By A Guest On the Operator's Property Does Not Violate Section 333.

Petitioners respectfully request that the Commission clarify that Section 333 does not prohibit a Wi-Fi network operator from managing its network on its premises, even when doing so causes "interference" to Part 15 devices used by guests on the operator's property. Part 15 of the Commission's rules permits the operation of low power radio frequency devices without an individual license from the Commission. As the Commission recently explained, "Part 15 rules are designed to ensure that there is a low probability that these devices will cause harmful interference to other users of the same or adjacent spectrum" because such devices generally "operate at very low power over relatively short distances, and often employ various techniques, such as dynamic spectrum access or listen-before-talk protocols, to reduce the interference risk to others as well as themselves."²⁰ To the extent a Wi-Fi operator's management of its network "interferes" with another Part 15 device operated by a guest on its property, the Commission should clarify that any such "interference" does not violate Section 333.

Enacted as part of the Federal Communications Commission Authorization Act of 1990 ("FCC Authorization Act"), Section 333 provides that "no 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."²¹ Many cases in which the Commission has found a Section 333 violation involved jammers (including cell phone jammers and GPS blockers), which the Commission has long determined to be

²⁰ 5 GHz Order ¶ 3

²¹ 47 U.S.C. § 333.

unlawful.²² Other decisions finding a violation of Section 333 involved interference with licensed radio operations by unlicensed radio operators or a licensed operator using equipment in violation of the FCC rules.²³

As far as Petitioners are aware, the FCC has never interpreted Section 333 to prohibit interference to Part 15 devices or found a violation of Section 333 based upon such interference. This is not surprising because such an interpretation of Section 333 would be legally unsustainable.²⁴

First, at the time of Section 333's enactment, the Communications Act did not address Part 15 devices, let alone authorize their use "under this chapter." In 1990 (the year Congress enacted Section 333), the Act's lone provision relating to operating a station in specified radio "services" without an individual station license was Section 307, which limited such operation to "the radio control service and the citizens band radio service."²⁵ Congress did not amend the Act

²² See, e.g., *In the Matter of George Conde*, Citation and Order, 27 FCC Rcd 12859 (Enf. Bur. 2012); *In the Matter of John A. Bering*, Citation and Order, 27 FCC Rcd 12846 (Enf. Bur. 2012).

²³ See, e.g., *In the Matter of David E. Perka, Annapolis, Maryland*, File Number: EB-07-CF-0119, DA 11-1584, Forfeiture Order, 26 FCC Rcd 13087 (2011); *Kevin W. Bondy*, Memorandum Opinion & Order, 28 FCC Rcd 1170 (Enf. Bur. 2013), *aff'g* Forfeiture Order, 26 FCC Rcd 7840 (Enf. Bur. 2011), *aff'g* Notice of Apparent Liability for Forfeiture, NAL/Acct. No. 200932900004 (Enf. Bur. rel. May 14, 2009).

²⁴ Almost a decade ago, the FCC's Office of Engineering and Technology ("OET") issued a public notice in which it reaffirmed the FCC's "exclusive authority to resolve matters involving radio frequency interference [RFI] when unlicensed devices are being used," including at so-called "multi-tenant environments ... such as hotels, conference centers, airports, and colleges and universities." *Commission Staff Clarifies FCC's Role Regarding Radio Interference Matters And Its Rules Governing Customer Antennas And Other Unlicensed Equipment*, Public Notice, DA 04-1844 (rel. June 24, 2004). However, OET did not indicate at that time (or at any time since) that interference to unlicensed devices in multi-tenant environments violates Section 333. Indeed, Section 333 is not even mentioned in OET's Public Notice.

²⁵ See Communications Amendments of 1982, 97 P.L. 259, § 113. The Telecommunications Act of 1996 expanded the services to include "the aviation radio service for aircraft stations operated on domestic flights when such aircraft are not otherwise required to

to expressly authorize “unlicensed” services generally until six years later when it adopted Section 332(c)(7), “Preservation of Local Zoning Authority,” as part of the 1996 Act.²⁶

Congress enacted subsequent amendments to the Act that referenced “unlicensed” use as part of the Balanced Budget Act of 1997 and the Twenty-First Century Communications and Video Accessibility Act of 2010.²⁷ However, Congress’s intent in enacting Section 333 must be divined at the time of the statute’s enactment, not years later.²⁸ Because Part 15 devices plainly were not “authorized by or under” the Communications Act when Section 333 was adopted, Congress could not reasonably have intended Section 333 to encompass Part 15 devices.

Second, that Congress did not intend Section 333 to prohibit interference to Part 15 devices is confirmed by the statute’s legislative history. In both the Senate and House reports accompanying the legislation, Congress indicated that Section 333 was intended to address the Commission’s concern about interference to certain types of radio communications services, namely: (i) “amateur, maritime, and citizens band radio” services; (ii) “public safety radio services”; and (iii) “private land mobile, and cable television” services.²⁹ Even though the

(footnote cont’d.)

carry a radio station; and (D) the maritime radio service for ship stations navigated on domestic voyages when such ships are not otherwise required to carry a radio station.” See 47 U.S.C. § 307; The Telecommunications Act of 1996, 104 P.L. 104, § 403(i) (“1996 Act”). Thus, this provision further codified the FCC’s authority to “license” certain stations “by rule” such that an individual station license would not be issued.

²⁶ 1996 Act, §704.

²⁷ Balanced Budget Act of 1997, 105 P.L. 33, § 3002 (adding 47 U.S.C. § 925 note); Twenty-First Century Communications and Video Accessibility Act of 2010, 111 P.L. 260, § 102 (amending 47 U.S.C. 610).

²⁸ *Perrin v. United States*, 444 U.S. 37, 42 (1979) (“A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning ... at the time Congress enacted the statute ...”); 2B Sutherland Statutory Construction § 50:1 (7th ed.) (“All legislation is interpreted in the light of the common law and the scheme of jurisprudence existing at the time of its enactment”).

²⁹ S. Rep. 101-215 at 7 (Nov. 19, 1989); H.R. Rep. 101-316, at 8 (Oct. 27, 1989).

FCC's Part 15 rules had been in place for more than 50 years when Section 333 was enacted in 1990, the legislative history of Section 333 is devoid of any mention of either Part 15 operations or Part 15 devices.³⁰ In short, nothing in the legislative history even remotely suggests that Congress adopted Section 333 to address interference to Part 15 devices or that the Commission believed that such interference was a problem Congress needed to address.

Section 333 also must be read in the context of the Commission's Part 15 rules. A primary operating condition for unlicensed devices under Part 15 is that the operator "must not cause harmful interference" and must "immediately correct the interference problem or to cease operation" should such harmful interference occur.³¹ In relevant part, "harmful interference" requires interruption to a "radiocommunications service" – a defined term the FCC has never construed to encompass Wi-Fi or any other Part 15 device.³² It would be anomalous – and legally suspect – for the Commission to interpret Section 333 to prohibit interference to a Part 15 device when such interference is not prohibited by the Part 15 rules under which the device is authorized to operate.

To be sure, the Part 15 rules require an operator "to accept whatever interference is received."³³ However, Section 333 makes unlawful the affirmative act of interfering with or

³⁰ *Revision of Part 15 Rules*, 4 FCC Rcd 3493, ¶ 2 (1989) (noting that the Commission's Part 15 rules were adopted in 1938 when "the Commission allowed devices employing relatively low level RF signals to be operated without the need for individual licensing as long as their operation caused no harmful interference to licensed services and the devices did not generate emissions or field strength levels greater than a specified level").

³¹ *5 GHz Order* ¶ 3

³² *See* 47 C.F.R. § 15.3(m); 47 C.F.R. § 2.1; *see also Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems*, 17 FCC Rcd 13522, ¶ 7, n.7 (2002) (because "Part 15 devices are not part of a 'service,' ... interference caused to a Part 15 device by another Part 15 device does not constitute harmful interference").

³³ *5 GHz Order* ¶ 3; 47 C.F.R. § 15.5(b); *see also Continental Airlines Petition for Declaratory Ruling Regarding the Over-The-Air Reception Devices (OTARD) Rules*,

causing interference “to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government.” Any failure by an operator of a Part 15 device to “accept” interference (in contrast to the operator affirmatively interfering with or causing interference) could not violate Section 333 under the plain terms of the statute.

Furthermore, extending Section 333 to apply to interference with Part 15 devices would lead to unintended and illogical consequences. For example, under an expansive construction of Section 333, a homeowner using her cordless telephone that interferes with a neighbor’s phone would be in violation of federal law and subject to an enforcement action under Section 333. The same would be true for a housewife whose use of a baby monitor device causes interference to a neighbor’s garage door opener. Congress could not have intended such absurd results.³⁴

Even assuming Section 333 governs interference to Part 15 devices (which is not the case), the Commission should clarify that a Wi-Fi network operator does not violate Section 333 when any interference (i) results from the use of FCC-authorized equipment in managing its network on its premises and (ii) affects Part 15 devices used by guests on the operator’s premises. Such clarification is appropriate for two reasons.

First, reputable manufacturers are marketing (and have marketed for some time) equipment authorized by the FCC, the intended purpose of which is to enable a Wi-Fi network operator to identify and mitigate interference by other Part 15 devices. As the Commission has observed, “A party seeking to market a Part 15 unlicensed device to the public must first comply

(footnote cont’d.)

Memorandum Opinion and Order, 21 FCC Rcd 13201, ¶ 30 (2006) (“*Continental Airlines Order*”).

³⁴ Because “willful” is defined as the “conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate” the law, 47 U.S.C. § 312(f)(1), the homeowner and the housewife face potential liability under an expansive interpretation of Section 333 as long as they knowingly operated the equipment in question (the cordless telephone and the baby monitor in this example) and such operation caused “interference” to another Part 15 device.

with the Commission's equipment authorization procedures, which, *inter alia*, *require a demonstration that the device complies with the Commission's rules.*"³⁵ Under the circumstances, a Wi-Fi network operator that purchases FCC-authorized equipment to manage its Wi-Fi network has a reasonable expectation that it would be acting lawfully when using such equipment in the manner intended.³⁶ Indeed, a Wi-Fi network operator would have no way of knowing that use of FCC-authorized network management equipment in the manner intended would be unlawful.³⁷

Second, interpreting Section 333 to prohibit interference to Part 15 devices operated by guests on the premises of a hotel or similar venue would be inconsistent with the FCC's OTARD rules. In 2006 the Commission extended its OTARD rules, which prohibit restrictions on property that impair the use of certain antennas, to unlicensed devices that operate under Part

³⁵ See *Amendment of Part 15 of the Commission's Rules to Amend the Definition of Auditory Assistance Device in Support of Simultaneous Language Interpretation*, Report and Order, 28 FCC Rcd 6658, ¶ 3 (2013) (citing 47 C.F.R. §§ 2.803, 2.901, 15.201(b)) (emphasis added).

³⁶ See *FCC v. Fox Television Stations, Inc.*, 132 S.Ct. 2307, 2317 (2012) (due process requires that "laws which regulate persons or entities must give fair notice of conduct that is forbidden" and that "regulated parties should know what is required of them so they may act accordingly").

³⁷ In the case of signal jammers, the FCC has released multiple advisories and public notices warning the public that the sale or use of such devices in the United States is unlawful. See, e.g., *Sale or Use of Transmitters Designed to Prevent, Jam or Interfere With Cell Phone Communications Is Prohibited In The United States*, Public Notice, DA 05-1176 (rel. June 27, 2005); FCC Enforcement Advisory – Cell Jammers, GPS Jammers, And Other Jamming Devices, DA 11-250 (rel. Feb. 9, 2011). Likewise, the FCC repeatedly has notified wireless Internet service providers of interference caused to Terminal Doppler Weather Radar by U-NII systems and devices. See, e.g., Memorandum from Julius Knapp, Chief, Office of Engineering and Technology, FCC, and P. Michele Ellison, Chief, Enforcement Bureau, FCC, to Manufacturers and Operators of Unlicensed 5 GHz Outdoor Network Equipment Re: Elimination of Interference to Terminal Doppler Weather Radar (TDWR) (dated July 27, 2010). By contrast, Petitioners are unaware of any similar warnings from the FCC about the use of Wi-Fi network management equipment that is the subject of this Petition.

15.³⁸ However, one of the conditions that must be satisfied in order for a Part 15 device to be covered by the Commission's OTARD rules is that "the antenna must be located on the property within the exclusive use and control of the antenna user where the user has a direct or indirect ownership or leasehold in the property."³⁹

With respect to a hotel or similar venue, neither staying guests nor meeting or convention attendees have any "direct or indirect ownership or leasehold" interest in the hotel's property. Rather, they are at most invitees or licensees who thus would enjoy no rights under the Commission's OTARD rules. Construing Section 333 to prohibit interference to Part 15 devices operated by guests of a hotel or similar venue would give such guests superior rights as compared to owners or lessors of property in their use of Part 15 devices, which would be nonsensical from a legal or policy standpoint.

For the foregoing reasons, the Commission should grant the Petition and declare that Section 333 does not prohibit a Wi-Fi network operator from managing its network on its premises, even when doing so causes interference to Part 15 devices used by guests on the operator's property.

B. In The Alternative, The Commission Should Initiate A Rulemaking To Amend Its Part 15 Rules To Specify The Interference To Part 15 Devices That Section 333 Prohibits.

To the extent the Commission declines to issue the requested declaratory ruling, it instead should initiate a rulemaking to modify its Part 15 rules to address the issues raised in this Petition. At the very least, if the Commission believes that Section 333 implicates interference to Part 15 devices, it must reconcile the use of the term "interference" in the statute with the term "harmful interference" in Part 15, which as currently defined does not encompass Part 15

³⁸ 47 C.F.R. § 1.4000; *Continental Airlines Order* ¶ 8.

³⁹ *Continental Airlines Order* ¶ 12 (citing 47 C.F.R. § 1.4000(a)(1)).

devices. Under the Administrative Procedure Act (“APA”), the Commission must conduct a notice and comment rulemaking when it modifies substantive rules or otherwise effects “a change in existing law or policy.”⁴⁰

Likewise, the APA compels the Commission to conduct a notice and comment rulemaking when it promulgates substantive or legislative rules, which are those that “grant rights, impose obligations, or produce other significant effects on private interests.”⁴¹ Because the Commission has never previously interpreted Section 333 to prohibit interference to Part 15 devices, doing so now would “substantively affect[] the public to a degree sufficient to implicate the policy interests animating notice-and-comment rulemaking.”⁴²

Whether and to what extent Wi-Fi network operators can manage their networks to monitor and mitigate interference raise important policy questions that affect a broad cross section of the public, including network operators, equipment manufacturers, not to mention

⁴⁰ *Alcaraz v. Block*, 746 F.2d 593, 613 (9th Cir. 1984) (quotations omitted); *U.S. Telecom Ass’n v. FCC*, 400 F.3d 29, 34-35 (D.C. Cir. 2005) (“[I]f an agency adopts ‘a new position inconsistent with’ an existing regulation, or effects ‘a substantive change in the regulation,’ notice and comment are required.”); *Sprint Corp. v. FCC*, 315 F.3d 369, 374 (D.C. Cir. 2003) (explaining that “new rules that work substantive changes in prior regulations are subject to the APA’s procedures.”).

⁴¹ *Batterton v. Marshall*, 648 F.2d 694, 701-02 (D.C. Cir. 1980) (citations omitted); *U.S. Telecom Ass’n*, 400 F.3d at 34 (“This court and many commentators have generally referred to the category of rules to which the notice-and-comment requirements do apply as ‘legislative rules’”); *Am. Mining Cong. v. Mine Safety & Health Admin.*, 995 F.2d 1106, 1109 (D.C. Cir. 1993) (explaining that legislative rules “have the force and effect of law”).

⁴² See, e.g., *Electronic Privacy Information Center v. U. S. Dep’t of Homeland Security*, 653 F.3d 1, 6 (D.C. Cir. 2011) (holding that decision by the Transportation Security Administration to screen airline passengers by using advanced imaging technology instead of magnetometers should have been the subject of notice-and-comment rulemaking before being adopted); *Time Warner Cable Inc. v. FCC*, 729 F.3d 137, 169 (2d Cir. 2013) (holding that the FCC’s standstill rule “is substantive and subject to the APA’s notice-and-comment requirements” because of “the substantive burden imposed by the standstill rule, the absence of an established FCC practice of issuing standstill orders in the program carriage context, and the uncertainty about the FCC’s authority to do so ...”).

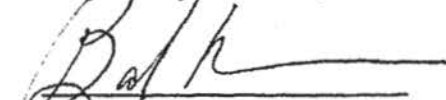
consumers. For example, is it appropriate for a university to limit a student's ability to use a Wi-Fi network for bandwidth intensive services and applications or to "interfere" with the student's access when he or she engages in such use? Similarly, should an airport authority be permitted to "interfere" with an unauthorized access point established by a visitor in the airport terminal that may be used to access travelers' mobile devices and obtain their confidential data without permission? Likewise, should it be permissible for a hotel to "interfere" with a guest who plugs an unauthorized access point into the hotel's wired network, which could pose a significant threat to the network's security? Finally, should operators of Wi-Fi networks have any ability to manage their networks to ensure reliable service by taking steps to mitigate network interference caused by unauthorized access points? These are important questions that can only be answered in a rulemaking.

Furthermore, in the absence of a rulemaking to address these questions, Wi-Fi network operators may have no choice but to take other steps to ensure the reliability and security of their networks without running afoul of Section 333. For example, a hotel could decide to prohibit guests from bringing Part 15 devices on the hotel's property. Alternatively, a hotel could limit the areas where Part 15 devices may be used, for example, by restricting their use to guest rooms or common areas. These measures – which no hotel would take lightly – could have significant public policy implications, which only underscores the need for the Commission to consider these issues in an industry-wide rulemaking.


IV. CONCLUSION

For the foregoing reasons, the Commission should grant the Petition and declare that the operation of FCC-authorized equipment by a Wi-Fi network operator to manage its network on its premises does not violate Section 333, even though such operation may "interfere with or cause interference to" a Part 15 device being used by a guest on the operator's property. In the alternative, the Commission should initiate a rulemaking proceeding to amend its Part 15 rules to specify what interference to Part 15 devices Section 333 prohibits.

Respectfully submitted,


Banks Brown
McDermott Will & Emery LLP
340 Madison Avenue
New York, NY 10173-1922
212 547 5488

*Counsel for the American
Hospitality & Lodging Association*


Bennett L. Ross
David Hilliard
Henry Gola
Wiley Rein LLP
1750 K Street, NW
Washington, DC 20006
(202) 719-7000

*Counsel for Marriott International, Inc. and
Ryman Hospitality Properties*

August 25, 2014

APPENDIX 1

APPENDIX 1

UNIVERSITY NETWORK MANAGEMENT TECHNIQUES

Name of University	Network Management Techniques
Appalachian State University	Appalachian State prohibits users from "unreasonably slow[ing] down the system by deliberately running wasteful jobs, playing games, engaging in non-productive or idle chatting, or sending mass mailings and chain letters." "The University will take appropriate action in response to user abuse," including "suspension or revocation of computing privileges" and "referral to law enforcement authorities." ⁱ
Brown University	Brown's computing department expects to "maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others." Brown reserves the right to "set limits on an individual's use of a resource through quotas, time limits, and other mechanisms." ⁱⁱ
California Institute of Technology	Cal Tech will not support or condone activities that "excessively consume" network resources. ⁱⁱⁱ
Columbia University	Columbia reserves the right monitor access to its information resources, communications on its network, and use of its systems and data. No user may "[o]bstruct University work by consuming excessive amounts of Network bandwidth and other System resources or by deliberately degrading performance of a computer." ^{iv}
Cornell University	Cornell does not allow "any activity that disrupts a system and interferes with other people's ability to use the system," such as "consuming more than your 'fair' share of resources." Cornell expressly includes as an example "running a file-sharing application such as KaZaA or Morpheus that slows down the network by consuming excessive bandwidth." ^v
Dartmouth College	Dartmouth states that members of its "community are entitled to a fair share of information resources." Dartmouth prohibits anyone on its network from "attempt[ing] to degrade Dartmouth or non-Dartmouth computer systems, networks, or personal computer performance, or to deprive other users . . . of information resources or authorized access" to any University- or individually owned computer. Dartmouth also "may restrict the availability of shared resources" when "necessary for the maintenance or mediated allocation of a system or network." ^{vi}
Duke University	For computers on Duke's network "where the utilization exceeds a daily threshold of 5 GB," the University will e-mail the owner of the computer, noting: bandwidth usage issues; tips on curbing outbound traffic usage; consequences for continued over-use; and information on how to request additional bandwidth if needed for academic or research projects. "After 5 such notices, the student's computer will have its outbound bandwidth restricted to 64 kb/s (kilobits per second) for the remainder of the semester." ^{vii}
Georgetown University	Georgetown prohibits users from "encroach[ing] on another's use of computer resources." Such activities include tying up resources to illegally share music, sending harassing messages, and using excessive amounts of storage. The University "reserves the right to limit access to its networks through University-owned or other computers, and to remove or limit access to material posted or

	distributed on University-owned computers.” ^{viii}
Harvard University	“In situations of high user demand that may strain available computer resources,” Harvard “reserves the right to restrict . . . or prohibit computer entertainment activities.” Harvard also reserves the right to “scan” its network “to assist in identifying and protecting against exploitable security vulnerabilities ... and to preserve network integrity and availability of resources.” ^{ix}
Indiana University	Indiana University prohibits “excessive use,” which it defines as existing when “a user or process has exceeded established limits placed on the service, or is consuming a resource to a level such that service to other users is degraded, or where the actions of a user could cause degradation if the user is permitted to continue the practice or activity.” The University may limit excessive use by establishing “per-user limits for the service that allow for shared use of limited resources; limitations on the types of processes that can be run on a service or resource; or identification of certain uses as adversely affecting the activities of others or adversely affecting system availability or performance.” ^x
Johns Hopkins University	Johns Hopkins states that “[u]ser[s] may not participate in activities that prevent the use or unduly degrade the performance of [network] resources.” Examples of these activities include “participation in activities that cause excessive strain on or interfere with the use of” network resources, such as distributing unsolicited bulk email, transferring multiple or large files, performing network scanning, and attaching to external sites to access video and audio streams not related to University work. The University will monitor “[a]ll network traffic, regardless of the source,” as necessary to “maintain[] the integrity and performance” of network resources, enforce University policies, and comply with local, state and federal law. ^{xi}
Massachusetts Institute of Technology	MIT takes seriously its “responsibility under the law to respond expeditiously to remove, or disable access to, [] material that is claimed to be infringing.” Although MIT does not affirmatively monitor its network for copyright violations, it does “monitor traffic patterns” for “intrusion detection.” ^{xii}
Northwestern University	Northwestern warns that “[a]ny person operating a network-intensive application or a defective computer” that “overloads networks, will be notified.” Steps also will be taken to protect the overall University network, including “disconnecting the offending computer system from the network until the problem is resolved. If the condition is an imminent hazard to the University network or disrupts the activities of others, then the offending computer system or the subnet to which it is attached may be disconnected without prior notice.” ^{xiii}
Ohio University	Ohio University advises that acceptable use “always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources.” Acceptable use “demonstrates respect for intellectual property, truth in communication, ownership of data, system security mechanisms, and individuals’ right to privacy and freedom of intimidation, harassment, and unwarranted annoyance.” The University “considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to test and monitor security, and copy and examine any files or information resident on university systems allegedly related to unacceptable use.” ^{xiv}
Princeton University	Princeton asks users to “be careful to avoid transmitting large amounts of data unnecessarily . . . [or] tying up shared computing resources for excessive game playing or other trivial applications.” Users with peer-to-peer sharing applications must limit uploads “to no more than one at a time (ideally, to zero),

	to prevent excessive use of Princeton's Internet bandwidth." ^{xv}
Stanford University	Stanford does not permit "network use or applications which inhibit or interfere with the use of the network by others," including using applications that "use an unusually high portion of the bandwidth for extended periods of time, thus inhibiting the use of the network by others." ^{xvi}
University of Chicago	The University warns users that they bear the responsibility for "avoiding any use that interferes with others' legitimate access to and use of University information technology." The University "may preserve, access, and disclose information from University information technology resources as permitted by law . . . to determine compliance with and enforce University policies and legal duties." ^{xvii}
University of Memphis	The University warns that "[i]nformation technology resources are finite and must be shared." Its "commitment to the principle of fair and equitable access for all users requires that users refrain from activities that compromise its overall ability to deliver IT services or that interfere with its ability to make IT resources available for all qualified users." Users also must not install or use unauthorized peer-to-peer sharing applications to distribute illicit illegal or dangerous material. When the University has reason to believe that a violation may have occurred, "he or she may immediately suspend information technology privileges for the involved user(s)." ^{xviii}
University of Pennsylvania	The University uses a priority system for certain applications when demand for network resources may exceed available capacity. The University may enforce these priorities by restricting or limiting usages of lower priority in circumstances where their demand and limitations of capacity impact or threaten to impact higher priority usages. ^{xix}
Washington University in St. Louis	Washington University instructs network users to "[a]void excessive use of computer resources" because "[t]hey are finite and others deserve their share." The University also states that some "[w]eb pages that are accessed to an excessive degree can be a drain on computer resources[.]" and except "where significant to the University's mission," the University may "ask that they be moved to a private Internet provider." The University also may empower systems managers or others to "suspend some or all privileges associated with computer use in cases of misuse or threat to the integrity of all or part of" the University's network resources. ^{xx}
Wesleyan University	Wesleyan prohibits "[u]ses of computer resources that may cause excessive network traffic or computing load," "illegal sharing of copyrighted material including music or video," and use of the network "to threaten or harass any person." University staff "are authorized to investigate alleged or apparent violations of University policy or applicable law" involving the network, and may suspend any account or limit account privileges, whether or not the account owner (the User) is suspected of any violation." ^{xxi}
Yale University	Yale classifies "[u]se that impedes, interferes with, impairs, or otherwise causes harm to the activities of others" as "inappropriate and prohibited." Users of Yale's network "must not deny or interfere with or attempt to deny or interfere with service to other users in any way," including by distributing unwanted mail or other unwanted messages. "Other behavior that may cause excessive network traffic or computing load is also prohibited." ^{xxii}

-
- ⁱ Appalachian State University IT Support Services, *Computer Use Policy*, at <http://support.appstate.edu/about/computer-use-policy> (last visited Aug. 14, 2014).
- ⁱⁱ Brown Information Technology, *Acceptable Use Policy*, at <http://www.brown.edu/information-technology/computing-policies/acceptable-use-policy> (last visited Aug. 14, 2014).
- ⁱⁱⁱ California Institute of Technology Information Network Systems & Services, *Network Policy*, at <http://www.imss.caltech.edu/node/142> (last visited Aug. 14, 2014).
- ^{iv} Columbia University, *Acceptable Usage of Information Resources Policy*, Oct. 2013, available at http://policylibrary.columbia.edu/files/policylib/imce_shared/sage_of_Information_Resources_Policy_FINAL_3.pdf.
- ^v Cornell IT, *What are some violations of Cornell University policy?*, at <http://www.it.cornell.edu/policies/university/privacy/responsible/violations.cfm#interfering> (last visited Aug. 14, 2014).
- ^{vi} Dartmouth University, *Dartmouth College Information Technology Policy: Allocation of Resources*, at <http://www.dartmouth.edu/comp/about/policies/general/itpolicy.html#allocation> (last visited Aug. 14, 2014).
- ^{vii} Duke Office of Information Technology, *ResNet bandwidth constraints: Addressing bandwidth utilization*, at <http://oit.duke.edu/net-security/network/resnet-policy.php> (last visited Aug. 14, 2014).
- ^{viii} Georgetown University Information Security Office, *Acceptable Use Policy*, at <http://security.georgetown.edu/technology-policies/acceptable-use> (last visited Aug. 14, 2014).
- ^{ix} Harvard University Information Technology, *Additional Policies from Harvard University Information Technology: Use of the Harvard Network*, at <http://huit.harvard.edu/pages/additional-policies-harvard-university-information-technology> (last visited Aug. 14, 2014).
- ^x Indiana University Policies, *Excessive Use of Information Technology Resources*, at <http://policies.iu.edu/policies/categories/information-it/it/IT-11.shtml> (last visited Aug. 14, 2014).
- ^{xi} The Peabody Institute of Johns Hopkins University, *Acceptable Use of IT Resources*, at <http://www.peabody.jhu.edu/it/policies/acceptableuse.html> (last visited Aug. 14, 2014).
- ^{xii} Massachusetts Institute of Technology, *Copyright at MIT: MIT's Policies with Respect to Copyright Infringement*, at <http://web.mit.edu/copyright/policy.html> (last visited Aug. 14, 2014); MIT Information Systems & Technology, *P2P Frequently Asked Questions (FAQ)*, at <http://kb.mit.edu/confluence/display/istcontrib/P2P+Frequently+Asked+Questions+%28FAQ%29#P2PFrequentlyAskedQuestions%28FAQ%29-MITNetwork> (last visited Aug. 14, 2014).
- ^{xiii} Northwestern University Information Technology, *Use of Student Residence Networks*, at <http://www.it.northwestern.edu/policies/resnet.html> (last visited Aug. 14, 2014).
- ^{xiv} Ohio University Policy & Procedure, *91.003: Computer and Network Use*, at <http://www.ohio.edu/policy/91-003.html> (last visited Aug. 14, 2014).
- ^{xv} Princeton University, *Policy on Use of Princeton University Information Technology*, Mar. 7, 2014, available at <http://www.princeton.edu/itpolicy/Princeton-IT-Policy-2013.pdf>.
- ^{xvi} Stanford Academic Computing Services, *Acceptable Use Policy*, at <http://acomp.stanford.edu/about/policy/aup> (last visited Aug. 14, 2014).
- ^{xvii} The University of Chicago IT Services, *The University of Chicago Policy on Information Technology Use and Access*, at <https://itservices.uchicago.edu/policies/acceptable-use-policy> (last visited Aug. 14, 2014).
- ^{xviii} The University of Memphis, *Acceptable Use of Information Technology Resources*, <http://umwa.memphis.edu/umpolicies/UM1535.htm> (last visited Aug. 14, 2014).
- ^{xix} University of Pennsylvania Information Systems & Computing, *Policy on Acceptable Use of Electronic Resources*, at <http://www.upenn.edu/computing/policy/aup.html#general> (last visited Aug. 14, 2014).
- ^{xx} Washington University in St. Louis, *Compliance and Policies: Computer Use Policy*, at <http://wustl.edu/policies/compolicy.html> (last visited Aug. 14, 2014).
- ^{xxi} Wesleyan University Information Technology Services, *Wesleyan Computer Usage Policy*, at <http://www.wesleyan.edu/its/policies/computerusage.html> (last visited Aug. 14, 2014).

^{xxii} Yale University, *1607 Information Technology Appropriate Use Policy*, at <http://policy.yale.edu/policy/1607-information-technology-appropriate-use-policy> (last visited Aug. 14, 2014).