**Before the**
**Federal Communications Commission**
**Washington, DC 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| M.C. Dean, Inc. | ) | File No.: EB-SED-15-00018428 |
| | ) | NAL/Acct. No.: 201632100003 |
| | ) | FRN: 0011134921 |

**NOTICE OF APPARENT LIABILITY FOR FORFEITURE**

**Adopted: October 28, 2015** **Released: November 2, 2015**

By the Commission: Commissioners Pai and O'Rielly dissenting and issuing separate statements.

## I. INTRODUCTION

1. We propose a penalty of $718,000 against M.C. Dean, Inc. (M.C. Dean) for apparently interfering with and disabling the operation of consumers' Wi-Fi devices at the Baltimore Convention Center (BCC). The Internet is a vital platform for economic growth, innovation, competition, and free expression. Wi-Fi is an essential access ramp to that platform. Wi-Fi networks have proliferated in places accessible to the public and consumers are increasingly establishing their own Wi-Fi networks by using mobile hotspots and their wireless data plans to connect Wi-Fi-enabled devices to the Internet. In this action, we address the practice of Wi-Fi blocking, which occurs when a Wi-Fi equipment operator intentionally disrupts the lawful operation of neighboring Wi-Fi networks. Wi-Fi blocking threatens to stymie wireless innovation and the availability of Wi-Fi as an important Internet access technology. Our action today advances the Commission's longstanding goal of ensuring that all authorized communications – including Wi-Fi transmissions – occur free of malicious disruptions.

2. Specifically, we find that M.C. Dean apparently repeatedly violated Section 333 of the Communications Act of 1934, as amended (Act)[1] by maliciously interfering with the operation of Wi-Fi networks at the BCC. Based on the evidence, we find that M.C. Dean blocked Wi-Fi devices on at least 26 days from November 2, 2014 to December 13, 2014 at the BCC.

## II. BACKGROUND

### A. Wi-Fi Generally

3. Wi-Fi is a technology that enables the wireless connection of low-power electronic devices.[2] Based on the 802.11 family of standards established by the Institute of Electrical and Electronics Engineers (IEEE), Wi-Fi networks enable devices such as laptop computers, tablets, video game consoles, and smartphones to connect to the Internet and to each other through wireless network

[1] 47 U.S.C. § 333.

[2] *See generally Implementation of Section 6002(B) of the Omnibus Budget Reconciliation Act of 1993*, Sixteenth Report, 28 FCC Rcd 3700, 3934, para. 376 (2013) (*Sixteenth Report*); *Google Inc.*, Notice of Apparent Liability and Forfeiture, 27 FCC Rcd 4012, 4014, para. 7 (Enf. Bur. 2012) (*Google NAL*). Today, most commonly used Wi-Fi equipment operates on unlicensed spectrum in the 2.4 GHz and 5.8 GHz bands, but other frequency bands may be used in the near future. *See* Radio-Electronics.com, *Wi-Fi / WLAN Channels, Frequencies, Bands & Bandwidths*, *available at* http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php (last visited July 31, 2015).

access points (APs).[3] According to the Wi-Fi Alliance,[4] more than 22,000 different Wi-Fi products have been certified since its inception in 1999, about two billion Wi-Fi capable devices were sold in 2013 alone, and by 2020, that number is expected to reach four billion annually.[5] Wi-Fi is particularly critical to the wireless broadband ecosystem, as developers, vendors, and manufacturers use Wi-Fi to link new types of products, systems, and devices that make our lives more efficient and comfortable. Though there are other wireless access technologies, such as Bluetooth, much of the developing "Internet of Things" depends on Wi-Fi connectivity.[6]

4. The most commonly-recognized wireless network access point is the Wi-Fi router that many consumers have in their homes, but a number of mobile devices can also serve as a wireless access point – or "hotspot" – that connects to the Internet through the mobile data network to which the consumer has subscribed.[7] Many mobile hotspots are stand-alone transmitting devices, typically the size of a deck of playing cards, and many smartphones sold today come with built-in Wi-Fi hotspot capabilities.[8] Consumers can use Wi-Fi-enabled devices, such as laptop computers or tablets, to wirelessly connect to these mobile hotspots and thereby access the Internet. In addition to personal hotspots, consumers may also access the Internet in a variety of businesses and public spaces through hotspots available for free or for a commercial fee.[9]

5. Wi-Fi communications follow a common protocol in establishing a connection, known as an "association" in Wi-Fi terminology, between an end-user client device (client) and an access point. This process occurs in three primary steps: the client first probes, then authenticates, and finally associates with the access point. Specifically, a "probe request" allows a client to determine what access points are available and to select the best one to use. An "authentication request" allows the client to establish its identity with the access point. Finally, an "association request" allows the authenticated client to transmit and receive data from the access point and connect to the network. When a client wishes to terminate the connection with an access point, or vice versa, the session is terminated through use of "deauthentication" and "disassociation" frames.[10] The transmission of deauthentication and disassociation frames in the ordinary course of ending a session is consistent with the 802.11 standard

[3] *Google NAL*, 27 FCC Rcd at 4014, para. 7; *see Revision of Part 15 of the Commission's Rules Regarding Operation in the 57-64 GHz Band*, Report and Order, 28 FCC Rcd 12517, 12520, para. 7, n.29 (2013); *Sixteenth Report*, 28 FCC Rcd at 3934, para. 376. We use the term "access point" or "AP" to refer to a device that has broadband access, either through a wired or wireless connection, and uses Wi-Fi to connect (and provide broadband access) to other Wi-Fi enabled devices, such as a laptop computer or tablet that is not otherwise connected to broadband. We refer to all of these Wi-Fi-enabled pieces of equipment – the access point and the laptop computer or tablet – as "Wi-Fi devices."

[4] The Wi-Fi Alliance® is a non-profit industry association that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability. *See* Wi-Fi Alliance, *Who We Are*, *available at* http://www.wi-fi.org/who-we-are (last visited July 31, 2015).

[5] Wi-Fi Alliance, *Wi-Fi Alliance® Celebrates 15 Years of Wi-Fi®* (Sept. 8, 2014), *available at* http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-celebrates-15-years-of-wi-fi (last visited July 31, 2015).

[6] *See*, *e.g.*, Craig J. Mathias, *Wi-Fi® and the Internet of Things: (Much) More than You Think* (Jan. 2, 2015), *available at* http://www.wi-fi.org/beacon/craig-mathias/wi-fi-and-the-internet-of-things-much-more-than-you-think (last visited July 31, 2015).

[7] *See generally Sixteenth Report*, 28 FCC Rcd at 3846, para. 225, n.701 (2013).

[8] *Id.*

[9] *Id.* at 3934–36, paras. 377–379.

[10] The IEEE standard 802.11-2012 protocol states that "[t]he deauthentication service is invoked whenever an existing authentication is to be terminated." "802.11-2012 – IEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," para. 4.5.4.3. The 802.11 protocol also provides that "[t]he disassociation service is invoked when an existing association is to be terminated." *Id.* at para. 4.5.3.4.

when used to terminate Wi-Fi communications between two devices within an existing network connection. The 802.11 protocols do not require any management, administrative control, or verification of these deauthentication and disassociation frames.[11]

6. "Wi-Fi blocking" occurs when a Wi-Fi equipment operator intentionally disrupts the lawful operation of neighboring Wi-Fi networks, including through the indiscriminate use of deauthentication frames to disrupt a Wi-Fi device's link to a Wi-Fi network other than the operator's network. The deauthentication protocol could be used to engage in Wi-Fi blocking in a variety of ways.[12] Wi-Fi blocking may be performed either manually or automatically using pre-set parameters.[13] In all cases, the blocking operator prevents the target device from establishing or maintaining a connection with a Wi-Fi network other than that of the blocking operator. Because deauthentication frames can be transmitted more quickly than a new link can be established, the blocking operator can ensure that the targeted device or devices are unable to establish or maintain a connection to a Wi-Fi network.

### B. Legal Framework

7. Key to the success of Wi-Fi is the ability of users to deploy authorized devices without a Commission license, thereby creating a "spectrum commons" – a frequency band in which spectrum can be shared successfully without Commission licensing of specific users. This is made possible by the Commission's imposition of power limits and requirements for each type of radio station that the Commission authorizes for manufacture, sale, and use in the band. As stated in the National Broadband Plan, this regulatory framework has been highly beneficial, producing "low barriers to entry and faster time to market, that have reduced costs of entry, spurred innovation and enabled very efficient spectrum

[11] *See id.* at para. 4.5.4.3 ("Deauthentication, and if associated, disassociation cannot be refused by the receiving STA [station] except when management frame protection is negotiated and the message integrity check fails."); *id.* at para. 4.5.4.9 (describing the optional robust management frame protection service).

[12] For example, the blocking operator can deauthenticate by sending a single deauthentication frame to the access point used by the target device while spoofing the target's MAC address in the "from" source address field. Alternatively, an operator can send the deauthentication frame directly to the target device, while spoofing the access point's MAC address in the frame. Or the operator can broadcast a single deauthentication to all devices, using a broadcast "to" destination address and spoofing the access point's address in the frame. *See* M.D. Aime et al., SECURITY AND PRIVACY IN ADVANCED NETWORKING TECHNOLOGIES 61–62 (Borka Jerman-Blazic & Wolfgang Schneider, eds.) (2004) (on file in EB-SED-15-00018428). In contrast to these actions, the use of deauthentication frames to terminate a connection on one's own network is routine and unobjectionable, akin to hanging up the phone. In addition, there are a variety of Wi-Fi blocking techniques capable of denying wireless service that do not rely on the use of deauthentication frames. *See* Kemal Bicakci & Bulent Tavli, *Denial-of-Service Attacks and Countermeasures in IEEE 802.11 Wireless Networks*, 31 COMPUTER STANDARDS & INTERFACES 931, 933-38 (2009) (on file in EB-SED-15-00018428).

[13] *See*, *e.g.*, Exhibit 19(e) at 119, 259, 366 (Xirrus User Manual) to Letter and Attachments from Bennett L. Ross, Wiley Rein LLP, Counsel to M.C. Dean, Inc., to Linda Nagel, Attorney Advisor, Spectrum Enforcement Division, FCC Enforcement Bureau (Apr. 17, 2015) (April 17 LOI Response) (on file in EB-SED-15-00018428) (describing the Xirrus system's various methods of classifying and deauthenticating "rogue" APs, both manual and automatic); *see also* Cisco Systems, Inc., *Rogue AP Detection under Unified Wireless Networks*, Document ID 70987 (Sept. 25, 2007), *available at* http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70987-rogue-detect.html (last visited August 19, 2015) ("once the rouge [sic] is detected you can now choose to either manually or automatically contain the detected rogue."). We understand "rogue" to mean a device that is not already authorized by the system that has detected and classified it, i.e., a device that may not belong on the classifying system's network. We observe that Cisco's instructions regarding containment of "rogue AP connected clients" state that it is "illegal to [contain] a legitimate AP in a neighboring WLAN." *See* Cisco Systems, Inc., *Rogue AP Containment*, Enterprise Mobility 4.1 Design Guide (Dec. 9, 2008), *available at* http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch4_Secu.html#wp1019262 (last visited July 31, 2015). It is our understanding that similar warnings have been contained in Cisco manuals for at least the past ten years.

usage."[14] As described below, Wi-Fi blocking threatens to disrupt the spectrum commons and violates the Act.

### 1. Wi-Fi Operates Under Part 15 of the Commission's Rules

8. The operation of Wi-Fi devices is regulated by Part 15 of the Commission's rules, which governs the use and marketing of low-power, unlicensed "intentional radiators."[15] These intentional radiators include not only Wi-Fi mobile hotspots, but a plethora of other devices, including cordless phones, baby monitors, garage door openers, wireless home security systems, and keyless automobile entry systems. Such devices are considered "unlicensed" because the Commission neither requires an operator to obtain an individual license from the Commission to use them nor licenses the operators by rule under its Section 307(e) authority.[16]

9. Unlicensed use of spectrum is a critical component of the Commission's national spectrum policy. Unlicensed devices generally operate at relatively low power on frequencies shared by many other users.[17] The Part 15 rules provide substantial flexibility in the types of unlicensed devices that can be operated. With regard to Wi-Fi devices, the Commission authorizes devices such as those used by M.C. Dean to operate in the 2.4 GHz and 5.8 GHz bands pursuant to Section 15.247 of its rules.[18] This rule section specifies a number of technical parameters for Wi-Fi device operations, including the operating frequency, modulation technique, channel bandwidth, antenna gain limits, and maximum transmitter power output.[19]

### 2. No Wi-Fi User has Greater Rights than Another Wi-Fi User

10. Wi-Fi devices operate on frequencies shared with other unlicensed devices; their rights are limited to facilitate sharing.[20] These limits are established both in the Act and the Commission's rules. Section 333 of the Act, which Congress enacted in 1990 to protect radio communications from willful or malicious interference,[21] provides broadly 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 Act or operated by the United States Government."[22] Thus, all Wi-Fi devices are prohibited

[14] Federal Communications Commission, *Connecting America: The National Broadband Plan* at 95 (2010), *available at* http://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf (last visited July 31, 2015); *see* Federal Communications Commission, Spectrum Policy Task Force, Report, ET Docket No. 02-135, at 22 (2002), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-228542A1.pdf (last visited July 31, 2015); Kenneth R. Carter et al., *Unlicensed and Unshackled: A Joint OSP-OET White Paper on Unlicensed Devices and Their Regulatory Issues* at 45 (OSP Working Paper No. 39, 2003), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-234741A1.pdf (last visited July 31, 2015).

[15] *See* 47 C.F.R. §§ 15.1–15.717; *Revision of Part 15 of the Commission's Rules Regarding Operation in the 57-64 GHz Band*, 28 FCC Rcd at 12518, para. 4 (Part 15 permits operation of radio frequency devices without an individual license and sets forth the technical rules for such operation).

[16] *See* 47 U.S.C. § 307(e) (providing that the Commission may, by rule, authorize the operation of radio stations in certain services without requiring individual licenses).

[17] *Unlicensed Operation in the TV Broadcast Bands*, First Report and Order and Further Notice of Proposed Rulemaking, 21 FCC Rcd 12266, 12268, para. 4 (2006).

[18] 47 C.F.R. § 15.247.

[19] The maximum permitted power level for a Wi-Fi device is one Watt. *Id.*

[20] *See* 47 C.F.R. §§ 15.215–15.257 (establishing radiated emission limits and other operational controls to avoid interference).

[21] *See* H.R. Rep. No. 101-316, at 13 (1989) (noting that Section 333 was intended "to prohibit the willful or malicious interference with radio communications, including government communications").

[22] 47 U.S.C. § 333.

from willfully or maliciously interfering with or causing interference to authorized communications, including other Wi-Fi transmissions. Part 15 of the Commission's rules also prescribes that operation of unlicensed devices is "subject to the condition[ ] that no harmful interference is caused."[23] The Part 15 rules define "harmful interference" as "[a]ny emission, radiation or induction that endangers the functioning of a radio navigation service or other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communications service operating in accordance with this chapter."[24]

11. The Enforcement Bureau (Bureau) has repeatedly and consistently warned against causing intentional interference, including to Wi-Fi transmissions. A 2011 Enforcement Advisory stated that the prohibition against devices that "intentionally block, jam, or interfere with authorized radio communications" includes Wi-Fi.[25] Similarly, another Enforcement Advisory issued in 2012 reiterated that devices should not be used that interfere with authorized communications, including by "preventing . . . Wi-Fi enabled device[s] from connecting to the Internet."[26] More recently, an Enforcement Advisory issued earlier this year warned that Section 333 prohibits blocking or disrupting the legitimate operation of personal Wi-Fi hotspots.[27]

12. The Bureau recently entered into consent decrees with the operator of a resort hotel and convention center and an Internet provider for conventions, meeting centers, and hotels, in proceedings involving Wi-Fi blocking.[28] In both proceedings, the companies, Marriott International, Inc. and Marriott Hotel Services, Inc. (collectively, Marriott) and Smart City Holdings, LLC (Smart City), employed Wi-Fi deauthentication to block consumers who sought to connect to the Internet using personal Wi-Fi hotpots.[29] Marriott admitted that the Wi-Fi users it blocked did not pose a security threat to the Marriott network.[30] Marriott agreed to settle the investigation by paying a civil penalty of $600,000 and establishing operating procedures to ensure that it does not engage in further Wi-Fi blocking.[31] Similarly, Smart City submitted no evidence that the deauthentication was done in response to a specifically identified security threat.[32] Smart City agreed to a civil penalty of $750,000 and to cease its Wi-Fi blocking activities.[33]

[23] *See* 47 C.F.R. § 15.5(b). The rule also provides that unlicensed transmitters must accept interference. *Id.* This condition allows all compliant devices equal access to the spectrum commons.

[24] 47 C.F.R. § 15.3(m).

[25] *Cell Jammers, GPS Jammers, and Other Jamming Devices; Consumers Beware: It is Unlawful to Use "Cell Jammers" and Other Equipment that Blocks, Jams, or Interferes with Authorized Radio Communications in the U.S.*, Public Notice, 26 FCC Rcd 1329 (Enf. Bur. 2011) (2011 Enforcement Advisory).

[26] *Cell Jammers, GPS Jammers, and Other Jamming Devices; Consumer Alert: Using or Importing Jammers is Illegal*, Public Notice, 27 FCC Rcd 2309 (Enf. Bur. 2012).

[27] *Warning: Wi-Fi Blocking is Prohibited; Persons or Businesses Causing Intentional Interference to Wi-Fi Hot Spots are Subject to Enforcement Action*, Public Notice, 30 FCC Rcd 387 (Enf. Bur. 2015).

[28] *Marriott Int'l, Inc.; Marriott Hotel Servs., Inc.*, Order and Consent Decree, 29 FCC Rcd 11760 (Enf. Bur. 2014) (*Marriott*); *Smart City Holdings, LLC et al*, Order and Consent Decree, 30 FCC Rcd 8382 (Enf. Bur. 2015) (*Smart City*).

[29] *Marriott*, 29 FCC Rcd at 11764, paras. 5–6; *Smart City*, 30 FCC Rcd at 8386, paras. 7–8.

[30] *Marriott*, 29 FCC Rcd at 11764, para. 6.

[31] *Id.* at 11764–65, paras. 10, 12, 17.

[32] *Smart City*, 30 FCC Rcd at 8386, para. 8.

[33] *Id.*, 30 FCC Rcd at 8387–88, paras. 14–16, 19.

### C. The Enforcement Bureau's Investigation of M.C. Dean

13. M.C. Dean is one of the largest electrical contracting companies in the country, with estimated sales of over $700 million in 2013.[34] M.C. Dean, which holds a common carrier license through a wholly-owned and controlled subsidiary, has provided telecommunications and Internet services, including Wi-Fi, to the BCC since at least October 2012.[35] During the period covered by this enforcement action, M.C. Dean provided and sold wireless Internet service to exhibitors and other attendees at the BCC for at least 10 events and at least 26 days, during which at least 43,000 exhibitors and attendees were present.[36] M.C. Dean charged $795 to $1,095 for access to the Wi-Fi it provided depending on whether the services were ordered in advance or on-site.[37]

14. On October 23, 2014, the Commission received an informal complaint from a company that provides private Wi-Fi networks for exhibitors at trade shows by shipping equipment to customers around the country.[38] The complainant stated in part that it had "just spent all morning arguing with M.C. Dean company who provides wireless [at the BCC] until they finally ceased sending de-auth signals to our router."[39] The complainant further stated that its AP logs showed M.C. Dean engaging in Wi-Fi blocking against its equipment at the BCC and that such blocking "is a carbon copy of the Marriott case."[40]

15. The next day, agents from the Bureau's Columbia Field Office visited the BCC during an exhibition and observed that Wi-Fi hotspots they established did not work inside the BCC, but did work outside of the BCC. Agents returned to the BCC on November 21, 2014, during another event and used specialized software to document that deauthentication packets were sent to Wi-Fi hotspots established by the agents. Agents made a third visit to the BCC on December 6, 2014, while two events were taking place, and again documented deauthentication packets sent to Wi-Fi hotspots they established.

---

[34] The Electrical Construction and Maintenance Magazine lists M.C. Dean as fifth out of the top 50 contractors with 2013 sales at $713,741,522. *Electrical Construction and Maintenance*, 2014 EC&M Top 50 Contractors, *available at* http://ecmweb.com/top-50-electrical-contractors/2014-ecm-top-50-contractors (last visited July 31, 2015).

[35] *See* Letter and Attachments from Bennett L. Ross, Wiley Rein LLP, Counsel to M.C. Dean, Inc., to Linda Nagel, Attorney Advisor, Spectrum Enforcement Division, FCC Enforcement Bureau, at 8 (Apr. 3, 2015) (April 3 LOI Response) (on file in EB-SED-15-00018428); April 17 LOI Response at 4. M.C. Dean holds two Industrial/Business Pool, Conventional Radio Licenses issued by the Commission (call signs WQKK749 and WPOY806) and its wholly-owned subsidiary, OpenBand of Virginia, LLC, holds an authorization to provide domestic, interstate communications services pursuant to Section 63.01(a) of the Commission's rules. *See* April 3 LOI Response at 7, 15. Another wholly-owned subsidiary, OpenBand Multimedia, LLC, holds a certification to operate an open video system pursuant to Section 76.1502 of the Commission's rules. *Id*.

[36] *See* Letter from Bennett L. Ross, Wiley Rein LLP, Counsel to M.C. Dean, Inc., to Bruce Jacobs, Chief, Spectrum Enforcement Division, FCC Enforcement Bureau, at Exhibit 37 (July 27, 2015) (Supplemental July 27 LOI Response) (on file in EB-SED-15-00018428) (stating the events had an estimated attendance from 150 to as many as 15,000).

[37] April 17 LOI Response, Attachment 1-17, Attachment 17. In addition to the BCC, M.C. Dean provides wireless Internet services at the Greater Richmond Convention Center in Virginia, but the company states that it did not engage in Wi-Fi blocking at that venue. *Id.* at 33.

[38] *See* COMPLAINT: EB-SED-14-00017551 (dated Oct. 23, 2014) (on file in EB-SED-15-00018428).

[39] *Id.*

[40] *Id.* The complainant also stated that M.C. Dean's IT manager "admitted they routinely block 'unauthorized' 'rogue' SSID's [sic]." *Id.* An SSID, or Service Set Identifier, is a sequence of characters that uniquely names a wireless local area network and allows stations to connect to the network when multiple independent networks operate in the same area.

16. During the December 6, 2014, inspection, agents spoke to an M.C. Dean employee and were told that all but two Wi-Fi channels were "restricted" by M.C. Dean at the BCC.[41] The M.C. Dean employee said that access to the "restricted" Wi-Fi channels would require paying M.C. Dean a fee of $795 in advance or $1,095 on the day of the event. The M.C. Dean employee further said that without proper access credentials provided by M.C. Dean, its system would continually deny a user Wi-Fi access. The agents subsequently inspected M.C. Dean's network management equipment and determined that the system used Xirrus hardware and software, backed up by Cisco equipment. Following receipt of the complaint and the agents' inspections, the Bureau's Spectrum Enforcement Division undertook an extensive investigation that included sending several Letters of Inquiry to M.C. Dean[42] and reviewing the company's written responses.[43]

17. In response to the Bureau's investigation, M.C. Dean admitted that it deployed deauthentication equipment at the BCC from October 2012 until December 13, 2014, and that it used an auto-block feature that automatically detected and indiscriminately deauthenticated any unknown AP.[44] Specifically, M.C. Dean's responses revealed that it deployed a Xirrus platform at the BCC with an auto-deauthentication function that M.C. Dean affirmatively turned on when it started using the system.[45] The Xirrus User Manual calls the auto-block function employed by M.C. Dean the "'shoot first and ask questions later' mode."[46] According to the manual, "[t]he Advanced RF Settings window allows you to set up Auto Block parameters so that unknown APs get the same treatment as explicitly blocked APs."[47]

[41] The employee also said the agents could connect to the free Wi-Fi offered at the BCC. However, M.C. Dean only offered free Wi-Fi in the BCC's "public lobby areas." April 17 LOI Response, Attachment 1-17.

[42] *See* Letter from Bruce D. Jacobs, Chief, Spectrum Enforcement Division, FCC Enforcement Bureau, to Mr. William H. Dean, Chief Executive Officer, M.C. Dean, Inc. (Mar. 4, 2015) (on file in EB-SED-15-00018428); Letter from Bruce D. Jacobs, Chief, Spectrum Enforcement Division, FCC Enforcement Bureau, to Mr. William H. Dean, Chief Executive Officer, M.C. Dean, Inc. and Bennett L. Ross, Wiley Rein LLP, Counsel to M.C. Dean, Inc. (June 23, 2015) (on file in EB-SED-15-00018428); Letter from Bruce D. Jacobs, Chief, Spectrum Enforcement Division, FCC Enforcement Bureau, to Mr. William H. Dean, Chief Executive Officer, M.C. Dean, Inc. (July 20, 2015) (on file in EB-SED-15-00018428).

[43] *See* April 3 LOI Response; April 17 LOI Response; Letter and Attachments from Bennett L. Ross, Wiley Rein LLP, Counsel to M.C. Dean, Inc., to Jason Koslofsky, Attorney Advisor, Spectrum Enforcement Division, FCC Enforcement Bureau (June 30, 2015) (June 30 LOI Response) (on file in EB-SED-15-00018428); Letter and Attachments from Bennett L. Ross, Wiley Rein LLP, Counsel to M.C. Dean, Inc., to Jason Koslofsky, Attorney Advisor, Spectrum Enforcement Division, FCC Enforcement Bureau (July 27, 2015) (July 27 LOI Response) (on file in EB-SED-15-00018428); Supplemental July 27 LOI Response; Letter and Attachments from Bennett L. Ross, Wiley Rein LLP, Counsel to M.C. Dean, Inc., to Jason Koslofsky, Attorney Advisor, Spectrum Enforcement Division, FCC Enforcement Bureau (August 7, 2015) (August 7 LOI Response) (on file in EB-SED-15-00018428); Letter and Attachments from Bennett L. Ross, Wiley Rein LLP, Counsel to M. C. Dean, Inc., to Jason Koslofsky, Attorney Advisor, Spectrum Enforcement Division, FCC Enforcement Bureau (August 14, 2015) (August 14 LOI Response) (on file in EB-SED-15-00018428); Letter from Bennett L. Ross, Wiley Rein LLP, Counsel to M. C. Dean, Inc., to Chairman Wheeler, Commissioner Clyburn, Commissioner Rosenworcel, Commissioner Pai, and Commissioner O'Reilly, FCC (Sept. 29, 2015) (September 29 Letter) (on file in EB-SED-15-00018428). M.C. Dean requested confidential treatment for certain information it provided in its April 17 LOI Response. *See* April 17 LOI Response 1. That request for confidentiality remains pending.

[44] *Id.* at 19–20; *see id.* at Exhibit 19(e) at 366–367 (Xirrus User Manual).

[45] April 17 LOI Response at 13–14. M.C. Dean refers to the system it employed at the BCC as the "Xirrus platform," while the Xirrus User Manual refers to the system as the "Array" and as the Xirrus Management System (XMS). Xirrus User Manual at 2. For the sake of consistency, we will refer to the deauthentication system used by M.C. Dean as the Xirrus platform or M.C. Dean's system.

[46] Xirrus User Manual at 366.

[47] *Id.* The Xirrus platform also lets the user detect and manually classify a particular AP as "Blocked," "so that the [Xirrus platform] will take steps to prevent stations from associating with the blocked AP." *Id*. at 259.

M.C. Dean set up the Xirrus platform to send deauthentication frames to any unknown AP that it detected outside of the "Auto Block" parameters.[48] When M.C. Dean classified an AP as Blocked, the Xirrus platform sent deauthentication signals to the AP, which "ha[d] the effect of disconnecting all of a Blocked AP's client devices approximately every 5 to 10 seconds," rendering the Blocked AP "frustratingly unusable."[49]

18. After receiving a request for Wi-Fi blocking records at the venues it serves, M.C. Dean claimed that it could locate only one record from a June 16, 2014, science conference at the BCC attended by an estimated 6,600 people.[50] The record lists 357 APs that the Xirrus Platform detected and classified as Blocked over 24 hours.[51] The blocked devices associated with the blocked APs included many smartphones and even Wi-Fi devices likely located outside the convention center.[52] For example, the record suggests that the auto-block function of M.C. Dean's system penetrated outside the BCC and targeted hotspots established by passing cars and buses for deauthentication.[53]

19. M.C. Dean claims without specific support that it used deauthentication to "detect and prevent malicious attacks on the wireless network and improve network security and reliability."[54] M.C. Dean also claims without support that its auto-blocking would have been limited because it would not

[48] *Id.* at 366 ("Auto blocking provides two parameters for qualifying blocking so that APs must meet certain criteria before being blocked. This keeps the [system] from blocking every AP that it detects.").

[49] *Id.* ("If you classify a rogue AP as blocked . . ., then the [Xirrus platform] will take measures to prevent stations from staying associated to the rogue. When the monitor radio is scanning, any time it hears a beacon from a blocked rogue it sends out a broadcast 'deauth' signal using the rogue's BSSID [basic service set identifier] and source address. This has the effect of disconnecting all of a rogue AP's clients approximately every 5 to 10 seconds, which is enough to make the rogue frustratingly unusable.").

[50] April 17 LOI Response at 21; *id.* at Exhibit 22(e) (XMS Reports Rogue List); *see* Supplemental July 27 LOI Response, Exhibit 37 (providing estimated attendance of 6,600 at 2014 American Society for Mass Spectrometry Conference).

[51] XMS Reports Rogue List at 1. The record lists other information for each AP, including the SSID, the "Vendor ID," the IP address, the apparent location where the AP was detected in the BCC, the security of the AP, the channel the AP was operating on, the Received Signal Strength Indicator value of the AP, and when the AP was first and last detected by the M.C. Dean system. *Id.* at 2.

[52] Every AP with an SSID that includes the word "iPhone" is classified as "Blocked," as is every AP with a "Vendor ID" identified as "Ford Motor" or "HTC," and almost all APs with a "Vendor ID" identified as "Samsung." *See generally* XMS Reports Rogue List. Two Samsung devices are classified as Unknown. Per the Xirrus User Manual, the system would have deauthenticated those devices as well. *See* Xirrus User Manual at 366.

[53] The fact that Ford Motor equipment appeared on the XMS Reports Rogue List suggests that M.C. Dean's system attempted to deauthenticate hotspots established by Ford cars driving past or otherwise outside the BCC that used Ford's Sync technology. Several SSIDs for "Bolt Bus" and "Go Buses" also indicate that M.C. Dean's system may have targeted APs for deauthentication outside of the BCC. XMS Reports Rogue List at 48, 175, 198, 199. Additionally, the report shows that M.C. Dean's system also detected Wi-Fi networks at hotels near the BCC, but such networks were generally identified as Approved and were apparently not targeted for deauthentication by M.C. Dean. *Id.* at 3, 6, 22 (several APs with SSID "Sheraton_WIFI" and "Hyatt Guest" are identified as Approved). APs associated with restaurants near the BCC also appear to have been detected but identified as Approved. *See id.* at 118 (AP named "Pratt Street Ale House" is identified as "Known").

[54] April 17 LOI Response at 13–14. The only arguable support that it provides is a cursory chart that claims to summarize "Intrusion and Threats Data" collected in December 2014 and February 2015. There is no documentation for the chart or its contents or any discussion of how its use of Wi-Fi blocking was directed at any such threats, let alone how it might have needed to block every Wi-Fi network point in the vicinity of the Baltimore Convention Center in order to secure its own network. *Id.* at 16-18, Exhibit 20(c).

have included certain brands of equipment or certain SSIDs,[55] that it left unblocked two of the over dozen typically-available Wi-Fi channels,[56] and that signal propagation limits may have limited the effectiveness of its Wi-Fi blocking attempts.[57] In sum, M.C. Dean claims that it wanted to "balance its contractual obligations to offer reliable and secure wireless services at the BCC with the ability of guests to use personal Wi-Fi hot spots when visiting the venue."[58]

20. M.C. Dean argues that its use of deauthentication "does not constitute 'interference' within the meaning of section 333" and the Act does not prohibit interference to Part 15 devices.[59] M.C. Dean claims that the Commission has made a distinction between "reasonable network management" and prohibited "interference," citing without explanation two Notices of Proposed Rulemaking regarding the use of cell phones in prisons and on airplanes.[60]

21. M.C. Dean argues the Commission has only applied Section 333 to a limited set of circumstances that does not include Wi-Fi blocking.[61] M.C. Dean states the equipment it used at the BCC "has been authorized by the Commission pursuant to section 302 of the [Act]" and was not operating on unauthorized frequencies or at unauthorized power levels.[62] Finally, M.C. Dean argues that, as a matter of due process, it did not receive "fair notice of the conduct that is forbidden" because its equipment is not a "jammer," Enforcement Advisories "do not represent decisions of the Commission," and only recent Enforcement Advisories warned that Section 333 prohibits willful and malicious interference to Part 15 devices.[63]

---

[55] M.C. Dean states that it "whitelisted" Wi-Fi equipment and "MiFi" devices from "the most prominent network manufacturers, including Cisco, Ruckus, Aruba, and Sierra" and it "whitelisted" certain SSIDs when an attendee at the BCC "had issues connecting to the Internet using a particular wireless transmitter." *Id.* at 15. The fact that M.C. Dean resolved connection issues by whitelisting SSIDs to stop deauthentication shows that deauthentication actually took place at the BCC as the result of M.C. Dean's use of the auto-block function on the Xirrus platform.

[56] *Id.* (claiming M.C. Dean did not auto-block for "devices operating on channel 1 on 2.4 GHz and channel 36 on 5GHz"). "Whitelisting" one channel in each band would not have decreased the likelihood of blocking. M.C. Dean offers no evidence that any device that was blocked by M.C. Dean would be capable of automatically finding the one channel in each band that was left unblocked. Such automatic capability does not appear to be standard among Wi-Fi devices and, if it were, it would still force all such devices to share a single channel that could become highly congested and perhaps unusable.

[57] *Id.* at 21–22. M.C. Dean claims that even if an AP was classified as Blocked, it may not have been deauthenticated if no device attempted to connect to it, or deauthentication may not work because of the "general RF activity at the BCC, the power setting of the AP, and the general environment in which the AP is operating in performing the deauthentication process (e.g., glass windows, concrete walls)." *Id.*

[58] September 29 Letter at 7.

[59] April 17 LOI Response at 29–30. M.C. Dean does not explain further how the plain language or legislative history of Section 333 support this contention. In any event, this argument is addressed in Section III.A.2 below.

[60] *Id.* at 29–30 (citing *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Notice of Proposed Rulemaking, 28 FCC Rcd 6603, paras. 14–20 (2013); *Expanding Access to Mobile Wireless Services Onboard Aircraft*, Notice of Proposed Rulemaking, 28 FCC Rcd 17132, para. 62 (2013)).

[61] *Id.* at 30 ("[T]he Commission has found a section 333 violation only in the following circumstances (i) the use of jammer (including cell phone jammers and GPS blockers), which the Commission has long determined to be unlawful . . . (ii) unlicensed radio operations that interfere with licensed radio operators . . . or (iii) the use of licensed equipment on unauthorized frequencies or at unauthorized power levels in a manner that interferes with other licensed equipment.") (citations omitted).

[62] *Id.*

[63] *Id.* at 30–31 (citing *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317, 183 L. Ed. 2d 234 (2012)).

## III. DISCUSSION

22. Based on the facts of this case, we find that M.C. Dean apparently violated Section 333 of the Act through its use of deauthentication frames to intentionally disrupt Wi-Fi devices that were lawfully and legitimately operating on shared spectrum, and propose a $718,000 forfeiture for such apparent violations.

### A. M.C. Dean's Wi-Fi Blocking Apparently Violated Section 333 of the Act

23. We find that M.C. Dean apparently repeatedly violated Section 333 of the Act by maliciously blocking Wi-Fi hotspot communications at the BCC in the past year. As discussed below, there are three key elements to our finding: (i) M.C. Dean engaged in Wi-Fi blocking; (ii) Wi-Fi blocking constitutes "malicious interference;" and (iii) Wi-Fi devices are "authorized station[s]." We also find that M.C. Dean's asserted motivation to prevent congestion and its reliance on security protocols do not justify its Wi-Fi blocking at the BCC. We similarly reject M.C. Dean's arguments that Wi-Fi blocking does not violate the law or that it did not have sufficient notice that Wi-Fi blocking was illegal.

#### 1. M.C. Dean Engaged in Wi-Fi Blocking

24. There is ample evidence that M.C. Dean engaged in widespread and indiscriminate Wi-Fi blocking during the past year. M.C. Dean admits that it deployed a system with an automatic Wi-Fi blocking capability at the BCC and enabled such automatic blocking until December 13, 2014.[64] Indeed, the Xirrus system manual called the aggressive auto-blocking function "'shoot first and ask questions later' mode."[65] In addition, Commission Field agents observed dropped Wi-Fi hotspot Internet connections and deauthentication packets sent by M.C. Dean's system during multiple visits to the BCC.[66] During those visits, an M.C. Dean employee said the company "restricted" all but two Wi-Fi channels at the BCC for all Wi-Fi networks and required payment to M.C. Dean for access to Wi-Fi.[67] The record provided by M.C. Dean, moreover, shows many instances of deauthentication over a 24-hour period during just one event at the BCC.[68] The record also shows that hotspots generated by typical smartphones would have been blocked, as shown by the near universal blocking of APs associated with iPhones or Samsung phones,[69] and suggests that M.C. Dean's system even targeted Wi-Fi devices located outside the BCC for deauthentication.[70] M.C. Dean's claims of limitations to its Wi-Fi blocking do not convince us that such blocking was not automatic and commonplace, rendering consumer mobile hotspots "frustratingly unusable."[71] M.C. Dean presents no evidence that any possible limitations materially impacted the likelihood that someone in the BCC attempting to use their own Wi-Fi hotspot would not have been blocked.[72] Finally, M.C. Dean concedes that it charged consumers hundreds of dollars or more

[64] *See supra* para. 17.

[65] *See id.*

[66] *See supra* para.15.

[67] *See supra* para. 16.

[68] *See supra* para. 18.

[69] *See supra* note 52.

[70] *See supra* note 53.

[71] *See supra* paras. 17, 19.

[72] M.C. Dean argues that an AP classified as "Blocked" on the XMS Reports Rogue List may not have actually been blocked. *See* April 17 LOI Response at 21–22. However, M.C. Dean offers no evidence that any particular AP was not blocked because it was "whitelisted" in some way or another. The XMS Reports Rogue List does not indicate if a particular AP was whitelisted. Moreover, it appears that at least some of the 357 APs were blocked because they were not within any of the "whitelist" parameters. The Xirrus User Manual contradicts M.C. Dean's claims that an AP classified as "Blocked" may not have been deauthenticated if it operated within a "whitelisted" parameter. *See* Xirrus User Manual at 366 ("If you classify a rogue AP as blocked . . . , then the [Xirrus platform] will take

(continued….)

to connect to its Wi-Fi network in the BCC,[73] and these charges clearly gave M.C. Dean a financial incentive to use its blocking capability. Thus, we conclude based on the totality of the evidence that M.C. Dean engaged in Wi-Fi blocking for several months during the past year. We leave our analysis of the frequency of M.C. Dean's blocking activity to Section III.B, below, in which we discuss the proposed forfeiture amount.

### 2. Wi-Fi Blocking Constitutes "Malicious Interference" Prohibited by Section 333 of the Act

25. Under the circumstances presented here, M.C. Dean's use of deauthentication frames with the intent to prevent third-party Wi-Fi devices from establishing or maintaining their own networks independent from M.C. Dean's Wi-Fi network constitutes "interfer[ing] with or interference to [] radio communications" within the plain meaning of Section 333 of the Act.[74] For purposes of Part 15, the Commission defines "harmful interference" as "[a]ny emission, radiation or induction that endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communications service operating in accordance with this chapter [Part 15]."[75] Deauthentication degrades, obstructs, and interrupts the radio communications between two third-party wireless networking devices. Section 333, moreover, not only prohibits one from causing "interference to" any radio communications, but also prohibits anyone from "interfer[ing] with" such communications.[76] The statute's two-part characterization of its prohibition against the disruption of radio communications constitutes a broad use of the concept of "interference," without limiting it to the radiofrequency (RF) component of a device's operations.[77] The Commission has, in other contexts, similarly interpreted the Section 333 concept of "interference" to include disruptions caused by actions other than RF interference. For example, in the amateur radio service context, the Commission found the "refusal by an operator to allow any other operator to talk" to be a violation of Section 333.[78] That communications are obstructed through the use of a standard protocol is no defense to Section 333. Here,

(Continued from previous page)
measures to prevent stations from staying associated to the rogue."). Regardless, the XMS Reports Rogue List identifies numerous APs classified as "Blocked" which were not on the "whitelisted" channels, and therefore would have been deauthenticated by M.C. Dean's system. *See e.g.*, XMS Reports Rogue List at 2 (AP with SSID "DBEDWiFi" operated on a blocked channel). Finally, any claim that limited signal propagation would have prevented deauthentication is belied by both the absence of any technical showing from M.C. Dean and the simple fact that if the AP was detected it presumably was in a position to be "Blocked." If the M.C. Dean system was able to receive a signal and detect the AP, then it only makes sense that M.C. Dean's system could transmit a signal that could be received by the AP.

[73] *See supra* para. 13.

[74] 47 U.S.C. § 333.

[75] 47 C.F.R. § 15.3(m).

[76] 47 U.S.C. § 333.

[77] It is a basic canon of statutory construction that we need to give meaning to both expressions ("interference" and "interfere with"). *See Miller v. Clinton*, 687 F.3d 1332, 1347 (D.C. Cir. 2012) (endorsing view that statutes should be construed "so that no provision is rendered inoperative or superfluous, void or insignificant") (quoting *Laurel Baye Healthcare of Lake Lanier, Inc. v. NLRB*, 564 F.3d 469, 472 (D.C. Cir. 2009) (internal quotation marks omitted). If we interpreted Section 333 to prohibit just RF interference, the phrase "interfere with" would be superfluous, which would be inconsistent with this canon of statutory interpretation. The broader view of what is prohibited – RF interference plus other acts that interfere with radio communications – explains why Congress used both expressions.

[78] *See, e.g.*, *Jack Gerritsen*, Forfeiture Order, 20 FCC Rcd 19256 (Enf. Bur. 2005); *John B. Genovese*, Order, 10 FCC Rcd 7594 (CIB 1995); *see also United States v. Baxter*, 841 F. Supp. 2d 378, 395 (D. Me. 2012) (affirming forfeiture imposed on amateur operator who refused to allow other operators to talk).

M.C. Dean would not allow mobile hotspots to connect to the Internet via a non-M.C. Dean approved network connection – thus intentionally obstructing lawful communication.

26. This broad interpretation of interference is consistent with the provision's legislative history, which includes the following specific examples of interference:

> intentional jamming, deliberate transmission on top of the transmissions of authorized operators already using specific frequencies in order to obstruct their communications, repeated interruptions, and the use and transmission of whistles, tapes, records, or other types of noisemaking devices to interfere with the communications or radio signals of other stations.[79]

Given the plain meaning of Section 333 and its legislative history, and consistent with the basic canon of statutory interpretation referenced above,[80] we conclude that Wi-Fi blocking constitutes a type of disruption to the use of spectrum that falls within the scope of Section 333's prohibition against interfering with or interference to radio communications.

27. Finally, the Wi-Fi blocking engaged in here appears to have been malicious, as M.C. Dean sought to cause, and in fact did cause, harmful interference to lawfully operated third-party networks. M.C. Dean established its blocking capability and used it with the specific intent to block the use of Wi-Fi by consumers not on its network. M.C. Dean knew that its system would cause interference to other Wi-Fi devices – in fact, that was the company's goal. As discussed elsewhere, M.C. Dean charged prices ranging from the hundreds to the thousands of dollars to exhibitors and others for Wi-Fi access that they should have been able to obtain directly through their own data plans. The company applied the "shoot first, ask questions later" setting on its equipment, leading to Wi-Fi blocking not only of persons in the BCC but even of passing Wi-Fi enabled vehicles. And M.C. Dean knowingly performed this conduct for over two years, including for two months after the Marriott consent decree.

28. Finding malicious interference here is consistent with other cases in which a party was found to have maliciously interfered with another when the interfering party deliberately sought to prevent the other person from transmitting communications signals on a given frequency. For example, the Commission has found malicious interference where an individual knowingly rendered his target's radios unusable by transmitting National Oceanic and Atmospheric Administration weather radio over the target's licensed channels. In that case, the interfering party "operated a radio . . . on the specific frequencies assigned and licensed by the Commission to [a third party], for the explicit and expressed purpose of prohibiting [the third party's] use of its licensed frequencies."[81] These actions were found to constitute repeated acts of intentional and malicious interference," as they "cut at the heart of the Commission's responsibilities to protect the nation's airwaves and regulate use of the spectrum."[82]

[79] H.R. Rep. No. 101-316, at 8.

[80] *See supra* note 77.

[81] *Kevin W. Bondy*, Forfeiture Order, 26 FCC Rcd 7840, 7841, 7845 paras. 5, 16 (Enf. Bur. 2011).

[82] *Id.* at 7845, para. 16; *see also Michael Guernsey*, Forfeiture Order, 30 FCC Rcd 7354, 7356 para. 5 (Enf. Bur. 2015) (malicious interference where violator deliberately played music and animal noises for the purpose of obstructing other amateur operators from communicating on the frequency); *Drew Buckley, Bay Shore, New York*, 29 FCC Rcd 7586, 7589, paras. 1, 10 (Enf. Bur. 2014) (finding "Mr. Buckley intentionally and maliciously interfered with frequencies used by [the Melville Fire District of New York]" where unauthorized transmissions on the fire department's frequencies disrupted dispatcher-firefighter communications"), *forfeiture ordered*, Forfeiture Order, 30 FCC Rcd 165 (2015).

### 3. Wi-Fi Devices Are "Stations" Within the Meaning of Section 333 of the Act

29. Section 333 applies to "any station licensed or authorized by or under [the] Act."[83] The devices at issue here – the APs and devices that were blocked – squarely fall within the meaning of "stations" as used in Section 333. Section 3 of the Act broadly defines "station" as "a station equipped to engage in radio communication or radio transmission of energy."[84] In addition, Congress's use of the modifier "any" before "station" in Section 333 further indicates its intent that the term "station" has a broad and inclusive meaning.[85] Congress provided several examples of radio services that would be protected from interference under Section 333, but did not limit the types of radio services or stations that would be protected.[86] In fact, the legislative history indicates the Congress did not intend to limit interference protection to a limited set of particular radio services, but rather intended Section 333 to provide a "general prohibition against intentional interference."[87] Thus, interpreting "any station" to encompass the Wi-Fi equipment at issue here, which is used to transmit communications and signals by radio, is consistent with the expansive language used in Sections 3 and 333 of the Act, the phrase's plain meaning, and Section 333's legislative history.

30. The Commission has consistently interpreted the definition of "station" to include Part 15 devices. For example, in its Ultra-Wideband Rulemaking in 2004, the Commission cited Section 303(f) of the Act, granting the Commission power to regulate to "prevent interference between stations," as authority for the Part 15 rules.[88] And, in a 2006 proceeding to preempt airport authorities from preventing an airline from installing Wi-Fi antennas in its passenger lounge, the Commission cited Section 303(d) of the Act, granting the Commission power to "[d]etermine the location of . . . stations," as its authority.[89] Accordingly, we conclude that the Wi-Fi devices that M.C. Dean apparently blocked at the BCC are "stations" within the meaning of Section 333 of the Act.

---

[83] 47 U.S.C. § 333.

[84] 47 U.S.C. § 3(42); *see* 47 U.S.C. § 3(40) ("For the purposes of this Act, unless the context otherwise requires . . . The term 'radio communication' or 'communication by radio' means the transmission by radio of writing, signs, signals, pictures, and sounds of all kinds, including all instrumentalities, facilities, apparatus, and services (among other things, the receipt, forwarding, and delivery of communications) incidental to such transmission.").

[85] *See, e.g.*, *Ali v. Fed. Bureau of Prisons*, 552 U.S. 214, 218–20 (2008) (noting that the use of "any" suggests a "broad meaning," and holding that the use of "any" to modify "other law enforcement officer" in a statute is "most naturally read to mean law enforcement officers of whatever kind.").

[86] *See* H.R. Rep. No. 101-316, at 8–9 (noting evidence of "willful and malicious interference to . . . the Amateur, Maritime, and Citizens Band Radio Services . . . and more isolated instances . . . in other services, including public safety, private land mobile, and cable television").

[87] *Id.* at 9; *see also id.* at 13 (broadly noting that the amendment is intended "to prohibit the willful or malicious interference with *radio communications*, including government communications") (emphasis added).

[88] *See Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems*, Second Report and Order and Second Memorandum Opinion and Order, 19 FCC Rcd 24558, 24591, para. 71 (2004); *see also id.* at 24593, para. 76 (explaining that authorizations of Part 15 devices pursuant to Part 2 of the Commission's rules are included among kinds of authorizations considered "station licenses" or "radio station licenses" for purposes of the Communications Act).

[89] *Continental Airlines; Petition for Declaratory Ruling Regarding the Over-the-Air Reception Devices (OTARD) Rules*, Memorandum Opinion and Order, 21 FCC Rcd 13201, 13216–17, para. 38 (2006). Our determination that Wi-Fi devices are stations is also consistent with IEEE 802.11. *See* IEEE 802.11-2007 (defining "station" as "[a]ny device that contains an IEEE 802.11-conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM)").

#### 4. M.C. Dean's Network Management and Notice Claims Do Not Justify its Wi-Fi Blocking

31. M.C. Dean claims without any evidentiary support that its blocking was necessary to provide a reliable and secure Wi-Fi service at the BCC.[90] But M.C. Dean was not authorized to block any lawful third-party Wi-Fi device under Section 333 of the Act, regardless of its desire to support its network. Wi-Fi operates in shared spectrum in which no user is entitled to block another in order to reduce congestion.[91] In addition, M.C. Dean misplaces its reliance on the federal cybersecurity guidelines it cites.[92] The recommendations in those guidelines that federal network operators have wireless intrusion detection and prevention systems do not authorize M.C. Dean (which is not a federal agency) to use those systems to send deauthentication frames to Wi-Fi users who are operating their stations as authorized to establish personal networks.[93] In any case, M.C. Dean failed to provide any evidence supporting its claim that its blocking activity actually targeted any devices that threatened the reliability or security of its Wi-Fi network or the users of its Wi-Fi network.[94] The record, rather, points to M.C. Dean using automatic blocking only to benefit itself commercially, to improve its system's performance, and to limit competition.

32. The legal arguments advanced by M.C. Dean to justify its Wi-Fi blocking are meritless. As addressed above, Wi-Fi blocking is "malicious interference" prohibited by Section 333, as demonstrated by the plain language and legislative history of the statute.[95] In contrast to M.C. Dean's claim that Section 333 is limited to interference caused by jammers and other unauthorized operations, the statute also prohibits malicious interference to any radio communications by an authorized station. Additionally, M.C. Dean has not explained how its indiscriminate Wi-Fi blocking could be considered a permissible network management tool. The company's automatic Wi-Fi blocking did not support the management of M.C. Dean's own network, but rather the prevention of others from operating their own networks apart from M.C. Dean's service. Moreover, as explained above,[96] M.C. Dean operates its Wi-Fi network on shared frequencies and its ability to operate on these frequencies is limited in that it must share the use of the frequencies with other devices lawfully operating on those frequencies. M.C. Dean, thus, may not operate its Wi-Fi network, including under the guise of network management, in a manner that unilaterally prevents consumers from using their own authorized devices from establishing mobile hotspots on shared spectrum through data services they already purchased. Further, the two Notices of Proposed Rulemaking cited by M.C. Dean without explanation do not alter this analysis and are irrelevant

[90] April 17 LOI Response at 15.

[91] *See supra* Section II.B.2.

[92] April 17 LOI Response at 17 (citing National Institute of Standards and Technology publications).

[93] The National Institute of Standards and Technology (NIST) publications are intended to provide federal agencies with guidelines and standards for information security and do not alter or supersede "the existing authorities" of "any other Federal official." *See* Guide to Securing Legacy IEEE 802.11 Wireless Networks at 1-1, Special Publication 800-48 Revision (July 2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf. The NIST publications do not authorize or condone a private company's indiscriminate use of Wi-Fi blocking, and in fact encourage network administrators to avoid performing actions that would harm "benign activity." *See* Guide to Intrusion Detection and Prevention Systems (IDPS) at 5-11, Publication 800-94 (Feb. 2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[94] April 17 LOI Response at 17–18. At most, M.C. Dean provides an unsubstantiated "summary" of the threats it claims it faced in December 2014 and February 2015. *Id.* at Attachment 20(c). This summary contains no explanation of the origin of the threat, including whether the threat originated from an independent third-party Wi-Fi network, or that blocking had any effect on the claimed threat.

[95] *See supra* Section III.A.2.

[96] *See supra* para. 10.

to the apparent Wi-Fi blocking violations at issue.[97] The "reasonable network management" practices discussed in the two Notices do not authorize or condone the type of indiscriminate Wi-Fi blocking that M.C. Dean engaged in at the BCC.[98]

33. M.C. Dean's claimed lack of notice is simply wrong. The Bureau has repeatedly and consistently warned, going back to 2011, that intentional blocking of Wi-Fi communications was unlawful and subject to enforcement action.[99] These warnings and the law are not limited to "jammers," or any other specific kind of technology or equipment. As clearly stated in the 2011 Enforcement Advisory, "it is a violation of federal law to use devices that intentionally block, jam, or interfere with authorized radio communications such as . . . Wi-Fi."[100] Here, regardless of the technology used, M.C. Dean did just that – intentionally blocked, jammed, and interfered with hundreds of consumers' Wi-Fi hotspots in violation of the law. Additionally, the Consent Decree with Marriott in October 2014 provided notice that the Commission could consider Wi-Fi blocking a violation of Section 333 of the Act.[101] Further, the fact that M.C. Dean purportedly failed to understand that Wi-Fi blocking violated the law does not excuse its apparent violations because the Commission "does not consider ignorance of the law a mitigating factor."[102]

### B. Proposed Forfeiture

34. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against any entity that "willfully or repeatedly fail[s] to comply with any of the provisions of [the Act] or of any rule,

[97] April 17 LOI Response at 29–30.

[98] The Commission's Notice of Proposed Rulemaking on mobile communications services aboard airborne aircraft is actually intended to *prevent* interference by redirecting signals in an airborne aircraft to new technology. *See Expanding Access*, 28 FCC Rcd at 17145**,** para. 31 ("Airborne Access Systems appear to be an effective means of providing airline passengers with mobile broadband connectivity, while preventing harmful interference to terrestrial wireless network."). It says nothing about indiscriminately blocking such signals. Similarly, nothing in the Notice of Proposed Rulemaking on contraband wireless devices in prisons expressly or implicitly authorizes indiscriminate blocking; to the contrary, it notes that signal jammers are not permitted under the Commission's rules. *Promoting Technological Solutions*, 28 FCC Rcd 6603, 6614, paras. 19–20 ("The Act prohibits any person from willfully or maliciously interfering with the radio communications of any station licensed or authorized under the Act . . . . Aside from the statutory constraints, wireless providers have indicated a preference for managed access solutions over jamming solutions, on the grounds that managed access 'can effectively prevent unauthorized communications without disrupting legitimate users.'").

[99] *See supra* para. 11. M.C. Dean points to no change in interpretation by the Commission of Section 333 that would deprive it of notice that malicious interference to Wi-Fi networks was prohibited. *See FCC v. Fox Television Stations, Inc.*, 132 S.Ct. 2307, 2318, 183 L.Ed.2d 234 (2012) (lack of fair notice where agency "changed course" with respect to its interpretation of a governing statute). Additionally, although it is not clear what M.C. Dean means when it states that Enforcement Advisories "do not represent decisions of the Commission," April 17 LOI Response at 30, the Enforcement Bureau is delegated to "[s]erve as the primary Commission entity responsible for enforcement of the Communications Act…." 47 CFR § 0.111(a). Enforcement Advisories are issued under delegated authority and "[e]xcept for the possibility of review, … have the same force and effect as actions taken by the Commission". *Id*. § 0.5(c); *see also id*. § 0.111(a)(19) (Enforcement Bureau delegated to "[e]ncourage cooperative compliance efforts"). Thus, an Enforcement Advisory can provide notice concerning what actions violate the Act.

[100] 2011 Enforcement Advisory, 26 FCC Rcd at 1329.

[101] The Marriott Consent Decree is discussed above. *Supra* para. 12. *Cf. FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121, at *15 (3d Cir. Aug. 24, 2015) (consent decrees entered into by the FTC with other companies regarding cybersecurity practices provided notice to Wyndham of what cybersecurity practices could violate 15 U.S.C. § 45(n)).

[102] *See, e.g.*, *Profit Enters., Inc.*, Forfeiture Order, 8 FCC Rcd 2846, 2846, para. 5 (1993) (citing *S. Cal. Broad. Co.*, Memorandum Opinion and Order, 6 FCC Rcd 4387 (1991)).

regulation, or order issued by the Commission."[103] Section 503(b)(2)(B) of the Act authorizes us to assess a forfeiture against M.C. Dean, a holder of a common carrier license,[104] of up to $160,000 for each day of a continuing violation, up to a statutory maximum of $1,575,000 for a single act or failure to act.[105] In exercising our forfeiture authority, we must consider the "nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[106] In addition, the Commission has established forfeiture guidelines; they establish base penalties for certain violations and identify criteria that we consider when determining the appropriate penalty in any given case.[107] Under these guidelines, we may adjust a forfeiture upward for violations that are egregious, intentional, or repeated, or that cause substantial harm or generate substantial economic gain for the violator.[108]

35. Section 1.80 of the Commission's rules and the Commission's *Forfeiture Policy Statement* set a base forfeiture of $7,000 for interference to authorized communications for each violation or each day of a continuing violation.[109] We have discretion, however, to depart from these guidelines, taking into account the particular facts of each individual case.[110]

36. We find that M.C. Dean apparently repeatedly violated Section 333 of the Act by maliciously blocking Wi-Fi hotspot communications at the BCC in the past year. As described above, the initial complaint, the three visits by FCC field agents, the automatic and indiscriminate Wi-Fi blocking technology that M.C. Dean admits to deploying from October 2012 to December 13, 2014, and M.C. Dean's own record of large numbers of consumer devices over a single 24-hour period at a BCC event in June 2014 all demonstrate a high likelihood that M.C. Dean engaged in Wi-Fi blocking whenever it was

[103] 47 U.S.C. § 503(b).

[104] M.C. Dean's wholly-owned and controlled subsidiary, OpenBand of Virginia, LLC, holds a common carrier license, which subjects M.C. Dean to the higher common carrier statutory maximum. *See* April 3 LOI Response at 7, 15; *supra para*. 13; *see also* M.C. Dean, Inc., *About M.C. Dean, Inc.*, *available at* http://www.mcdean.com/about/companies.htm (last visited September 1, 2015) ("OpenBand of Virginia, LLC (OpenBand) is a wholly owned subsidiary of M.C. Dean founded in 1999 by company CEO, Bill Dean, and several key colleagues. OpenBand is a licensed telecommunications carrier and a converged services provider, offering broadband communications packages throughout the MidAtlantic.").

[105] *See* 47 U.S.C. § 503(b)(2)(B); 47 C.F.R. § 1.80(b)(2). These amounts reflect inflation adjustments to the forfeitures specified in Section 503(b)(2)(B) ($100,000 per violation or per day of a continuing violation and $1,000,000 per any single act or failure to act). The Federal Civil Penalties Inflation Adjustment Act of 1990, Pub. L. No. 101-410, 104 Stat. 890, as amended by the Debt Collection Improvement Act of 1996, Pub. L. No. 104-134, Sec. 31001, 110 Stat. 1321, requires the Commission to adjust its forfeiture penalties periodically for inflation. *See* 28 U.S.C. § 2461 note (4). The Commission most recently adjusted its penalties to account for inflation in 2013. *See Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, 28 FCC Rcd 10785 (Enf. Bur. 2013); *see also* Inflation Adjustment of Monetary Penalties, 78 Fed. Reg. 49,370-01 (Aug. 14, 2013) (setting Sept. 13, 2013, as the effective date for the increases).

[106] 47 U.S.C. § 503(b)(2)(E).

[107] 47 C.F.R. § 1.80(b)(8), Note to paragraph (b)(8).

[108] *Id.*

[109] 47 C.F.R. § 1.80(b); *The Commission's Forfeiture Policy Statement and Amendment of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, Report and Order, 12 FCC Rcd 17087 (1997) (*Forfeiture Policy Statement*), *recons. denied*, 15 FCC Rcd 303 (1999).

[110] *Forfeiture Policy Statement*, 12 FCC Rcd at 17098–99, para. 22 (1997) (noting that "[a]lthough we have adopted the base forfeiture amounts as guidelines to provide a measure of predictability to the forfeiture process, we retain our discretion to depart from the guidelines and issue forfeitures on a case-by-case basis, under our general forfeiture authority contained in Section 503 of the Act").

providing service and there was an event at the convention center.[111] We find it reasonable to conclude that a violation apparently took place every day there was an event at the BCC within the past year and M.C. Dean sold Wi-Fi to the event planner or event exhibitors.[112] The evidence demonstrates that deauthentication undoubtedly took place when there were events held at the BCC.[113] M.C. Dean's submissions show that at least 10 events took place at the BCC on at least 26 days over the past year where M.C. Dean sold Wi-Fi service.[114]

37. Based on its account of the BCC events it served, we find that M.C. Dean blocked Wi-Fi devices at the BCC on at least 26 days. Consistent with 503(b) of the Act, Section 1.80 of the Commission's rules, and the *Forfeiture Policy Statement*, we begin our calculation with the base forfeiture of $7,000 for each of the 26 days, resulting in a total base forfeiture of $182,000 for M.C. Dean's apparent Wi-Fi blocking violations.

38. Given the totality of the circumstances, and consistent with the *Forfeiture Policy Statement*, however, we also conclude that a significant upward adjustment is warranted here. In this case, we upwardly adjust for M.C. Dean's ability to pay, the egregious nature of its violations in light of the importance of Wi-Fi capability to consumers, and the repeated and continuous nature of its violations.[115]

39. First, to ensure that a proposed forfeiture is not treated as simply a cost of doing business, the Commission has determined that large or highly profitable companies should be subject to proposed forfeitures that are substantially above the base forfeiture amount.[116] Industry publications state that M.C.

---

[111] *See supra* paras. 14–18, 24.

[112] This calculation may underestimate the number of violations that occurred in the past year given that the XMS Reports Rogue List apparently lists Wi-Fi networks classified as Blocked that were generated outside the BCC (e.g., "Ford Motor" equipment and "Bolt Bus" SSIDs), indicating deauthentication may have occurred even on days when no event occurred at the BCC. *See supra* para. 18, note 53; *see also* April 17 LOI Response at 19–20; August 14 LOI Response, Revised Exhibit 38. Indeed, M.C. Dean concedes "the Xirrus platform is in constant operation at the BCC, regardless of whether [M.C. Dean] is selling wireless Internet services on any particular day." September 29 Letter at 9.

[113] *See supra* para. 14–18. M.C. Dean indicates that it sold Wi-Fi on the days covered by the XMS Reports Rogue List, the complaint, and the Field visits when deauthentication apparently occurred. *See* August 14 LOI Response, Revised Exhibit 38.

[114] June 30 LOI Response, Exhibit 35; June 30 LOI Response, Exhibit 36; August 14 LOI Response, Revised Exhibit 38. M.C. Dean's last submission purported to show only 24 days of events where Wi-Fi was sold during the relevant time period. *See* August 14 LOI Response, Revised Exhibit 38. However, an analysis of public sources and other submissions by M.C. Dean show that 26 days of events occurred during the relevant time period where M.C. Dean sold Wi-Fi. *See* June 30 LOI Response, Exhibit 36 (exhibit shows that the events Whitman Coin and Collectibles and National Association for Gifted Children Annual Conference lasted longer than indicated on August 14 LOI Response, Revised Exhibit 38). Accordingly, we find that 26 days is the proper number of days on which to base the forfeiture amount.

[115] 47 U.S.C. § 503(b)(2)(E); 47 C.F.R. § 1.80(b)(8), Note to paragraph (b)(8).

[116] *See Forfeiture Policy Statement*, 12 FCC Rcd at 17099–17100, paras. 23–24 (cautioning all entities and individuals that, independent from the uniform base forfeiture amounts, the Commission will take into account the violator's ability to pay in determining the amount of a forfeiture to guarantee that forfeitures issued against large or highly profitable entities are not considered merely an affordable cost of doing business, and noting that such entities should expect the forfeiture amount set out in a Notice of Apparent Liability for Forfeiture against them may in many cases be above, or even well above, the relevant base amount); *AT&T Commc'ns*, Notice of Apparent Liability for Forfeiture, 30 FCC Rcd 856, 862, para. 14 (2015) (doubling base forfeiture based on company's ability to pay); *GCI Commc'ns Corp*., Notice of Apparent Liability for Forfeiture, 28 FCC Rcd 12991, 12994, para. 9 (Enf. Bur. 2013) (same); *Am. Movil, S.A.B. de C.V., Parent of Puerto Rico Tel. Co., Inc.*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 8672, 8676, para. 10 (Enf. Bur. 2011) (same); *see also Union Oil Co. of Cal*., Notice of

(continued….)

Dean had over $700 million in sales in 2013 and list M.C. Dean as one of the largest electrical contractors in the county.[117] Thus, to ensure that the forfeiture is an effective deterrent for M.C. Dean as well as to protect the interests of consumers, an upward forfeiture adjustment based on M.C. Dean's relative ability to pay is justified.

40. Second, M.C. Dean's blocking activities are a particularly egregious form of misconduct that warrants a substantial increase to the base forfeiture for unlawful interference provided in the Commission's rules. Wi-Fi blocking runs counter to fundamental Commission principles by stymieing wireless innovation, competition, and the availability of Wi-Fi as an important Internet access technology. By preventing consumers, including exhibitors and attendees, from using previously purchased devices and data plans to establish Wi-Fi hotspots, M.C. Dean forced them to pay anywhere from hundreds to thousands of dollars for Wi-Fi access that they should have been able to obtain directly through their data plans. Over 43,000 exhibitors and attendees were present at the events where M.C. Dean engaged in Wi-Fi blocking during the period covered by this enforcement action.[118] As described above, M.C. Dean affirmatively applied blocking criteria at the BCC that led to automatic blocking of lawful, off-the-shelf consumer devices operating at normal power levels.[119] Additionally, M.C. Dean's unlawful conduct continued for two and half months after release of the Marriott Consent Decree.[120] It was only after M.C. Dean became aware that it was being investigated by the Commission that it stopped Wi-Fi blocking.

41. Additionally, substantial evidence suggests that M.C. Dean's system detected and blocked some APs likely located outside of the BCC.[121] In the records provided by M.C. Dean, every AP associated with "Ford" and "Bolt Bus" was identified as Blocked, suggesting the M.C. Dean system deauthenticated Wi-Fi networks generated by Ford vehicles and Bolt Buses that passed the BCC.[122] This behavior, which impaired thousands of consumers' use of their lawful Wi-Fi devices is malicious and shows a pattern of conduct "suggest[ing] egregious misbehavior" warranting an upward forfeiture adjustment.[123]

42. Lastly, M.C. Dean admits it deployed its Wi-Fi blocking equipment for a substantial period outside the statute of limitations and that its blocking activities continued for an extended period of time, including blocking after the issuance of the Marriott Consent Decree. M.C. Dean turned on the auto-block function in October 2012, resulting in the deauthentication of Wi-Fi hotspots for BCC visitors for over two years before M.C. Dean claims it ceased its blocking activities in December 2014.[124] Such repeated or continuous violations also warrant a significant upward forfeiture adjustment.[125] Based on the

(Continued from previous page)
Apparent Liability for Forfeiture, 27 FCC Rcd 13806, 13810–11, paras. 10–11 (2012) (stating that proposed penalty must be large enough "to ensure that forfeiture liability is a deterrent and not simply a cost of doing business").

[117] *See supra* para. 13, note 34.

[118] *See supra* para. 13, note 36.

[119] *See supra* para. 17–18.

[120] *See supra* para. 12. The Marriott Consent Decree was released October 3, 2014 and M.C. Dean did not stop Wi-Fi blocking until December 13, 2014. *Id*. M.C. Dean employees were apparently aware of the Marriott Consent Decree when questioned by Field agents on December 6, 2014.

[121] *See supra* para. 18, note 53.

[122] *See id.*

[123] *Forfeiture Policy Statement*, 12 FCC Rcd at 17103, para. 35.

[124] *See supra* para. 17.

[125] *See AT&T Commc'ns*, 30 FCC Rcd at 861, para. 12 (finding upward forfeiture adjustment appropriate where a significant number of violations occurred for an extended period of time); *Sabrina Javani D/B/A EZ Business Loans*, Notice of Apparent Liability for Forfeiture, 27 FCC Rcd 7921, 7926, para. 9 (2012) ("[M]ore substantial penalties . . . are appropriate for persons and entities who engage in a significant number of violations."). Although a large
(continued….)

foregoing, an overall upward adjustment of $536,000 is warranted, bringing the overall proposed forfeiture amount to $718,000.

43. In applying the applicable statutory factors, we also consider whether there is any basis for a downward adjustment of the proposed forfeiture. Here, we find none. The malicious blocking of Wi-Fi hotspots is not a minor violation and M.C. Dean neither voluntarily disclosed its apparent violations nor ceased blocking until after the Bureau began its investigation.[126] While M.C. Dean previously maintained a history of compliance with the Commission's rules, we also find no reason to reduce the proposed forfeiture in light of the egregious, intentional, and repeated nature of the apparent violations.[127]

## IV. CONCLUSION

44. We have determined that M.C. Dean apparently repeatedly violated Section 333 of the Act and is apparently liable for a forfeiture of $718,000.

## V. ORDERING CLAUSES

45. Accordingly, **IT IS ORDERED** that, pursuant to Section 503(b) of the Act[128] and Section 1.80 of the Commission's rules,[129] M.C. Dean, Inc. is hereby **NOTIFIED** of its **APPARENT LIABILITY FOR A FORFEITURE** in the amount of seven hundred, eighteen thousand dollars ($718,000) for repeated violations of Section 333 of the Act.[130]

46. **IT IS FURTHER ORDERED** that, pursuant to Section 1.80 of the Commission's rules,[131] within thirty (30) calendar days of the release date of this Notice of Apparent Liability for Forfeiture, M.C. Dean, Inc. **SHALL PAY** the full amount of the proposed forfeiture or **SHALL FILE** a written statement seeking reduction or cancellation of the proposed forfeiture consistent with paragraph 49 below.

47. Payment of the forfeiture must be made by check or similar instrument, wire transfer, or credit card, and must include the NAL/Account Number and FRN referenced above. M.C. Dean, Inc. shall send electronic notification of payment to Jason Koslofsky at Jason.Koslofsky@fcc.gov, Pamera Hairston at Pamera.Hairston@fcc.gov and Samantha Peoples at Sam.Peoples@fcc.gov on the date said payment is made. Regardless of the form of payment, a completed FCC Form 159 (Remittance Advice)

(Continued from previous page)
number of these violations are not actionable due to the expiration of the statute of limitations period, the Commission has determined such violations may be relevant in determining adjustments to base forfeiture levels in setting the forfeiture amount. *See AT&T Commc'ns*, 30 FCC Rcd at 861–62, para. 13 (noting that the Commission can consider facts that occurred outside the statute of limitations period in assessing an appropriate forfeiture amount); *Enserch Corp.*, Forfeiture Order, 15 FCC Rcd 13551, 13554, para. 11 (2000) (same).

[126] *See* 47 C.F.R. § 1.80 (listing "good faith or voluntary disclosure" and "minor violation" as downward forfeiture adjustment criteria). As explained above, M.C. Dean's claimed ignorance of the law does not justify a downward adjustment. *See supra* para. 33.

[127] *TV Max, Inc. and Broadband Ventures Six, LLC d/b/a Wavevision, et al.*, Forfeiture Order, 29 FCC Rcd 8648, 8660, para. 24 (2014) (finding that the "egregious, intentional and repeated nature of TV Max's violations and TV Max's high degree of culpability present in this case easily outweigh TV Max's claimed history of no prior offenses.").

[128] 47 U.S.C. § 503(b).

[129] 47 C.F.R. § 1.80.

[130] 47 U.S.C. § 333.

[131] 47 C.F.R. § 1.80.

must be submitted.[132] When completing the FCC Form 159, enter the Account Number in block number 23A (call sign/other ID) and enter the letters "FORF" in block number 24A (payment type code). Below are additional instructions that should be followed based on the form of payment selected:

- Payment by check or money order must be made payable to the order of the Federal Communications Commission. Such payments (along with the completed Form 159) must be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank – Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.
- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. To complete the wire transfer and ensure appropriate crediting of the wired funds, a completed Form 159 must be faxed to U.S. Bank at (314) 418-4232 on the same business day the wire transfer is initiated.
- Payment by credit card must be made by providing the required credit card information on FCC Form 159 and signing and dating the Form 159 to authorize the credit card payment. The completed Form 159 must then be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank – Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

48. Any request for making full payment over time under an installment plan should be sent to: Chief Financial Officer – Financial Operations, Federal Communications Commission, 445 12th Street, S.W., Room 1-A625, Washington, DC 20554.[133] Questions regarding payment procedures should be directed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

49. The written statement seeking reduction or cancellation of the proposed forfeiture, if any, must include a detailed factual statement supported by appropriate documentation and affidavits pursuant to Sections 1.16 and 1.80(f)(3) of the Commission's rules.[134] The written statement must be mailed to the Office of the Secretary, Federal Communications Commission, 445 12th Street, S.W., Washington, DC 20554, ATTN: Enforcement Bureau – Spectrum Enforcement Division, and must include the NAL/Account Number referenced in the caption. The statement must also be e-mailed to Jason Koslofsky at Jason.Koslofsky@fcc.gov and Pamera Hairston at Pamera.Hairston@fcc.gov.

50. The Commission will not consider reducing or canceling a forfeiture in response to a claim of inability to pay unless the petitioner submits: (1) federal tax returns for the most recent three-year period; (2) financial statements prepared according to generally accepted accounting practices; or (3) some other reliable and objective documentation that accurately reflects the petitioner's current financial status. Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation.

[132] An FCC Form 159 and detailed instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

[133] *See* 47 C.F.R. § 1.1914.

[134] 47 C.F.R. §§ 1.16, 1.80(f)(3).

51. **IT IS FURTHER ORDERED** that a copy of this Notice of Apparent Liability for Forfeiture shall be sent by first class mail and certified mail, return receipt requested, to Bennett L. Ross, Wiley Rein LLP, Counsel to M.C. Dean, Inc., at 1776 K Street NW, Washington, DC 20006.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

**DISSENTING STATEMENT OF COMMISSIONER AJIT PAI**

Re: *M.C. Dean, Inc.*, File No. EB-SED-15-00018428.

Before the FCC can enforce rules, rules must exist. That's why I believe that the FCC should adopt rules that limit Wi-Fi blocking. Wi-Fi blocking occurs when a person uses an unlicensed Part 15 device to intentionally disrupt the operation of another unlicensed Part 15 device, such as a mobile hotspot that a consumer sets up to connect a Wi-Fi-enabled device to the Internet via his or her smartphone. I also believe that those rules should make clear that no person has *carte blanche* to intentionally disrupt another person's Wi-Fi connection.

Over a year ago, parties petitioned the FCC to enact such regulations.[1] They asked the FCC to establish clear rules of the road through an industry-wide rulemaking. As one might expect, commenters responding to the petition offered very different takes on what any such rules should look like. Some argued that Wi-Fi blocking should not be allowed under any circumstance.[2] Others argued that deauthentication is part of the IEEE 802.11 standard and should be permitted when necessary to ensure network security, such as to shut down access-point spoofing or other cyberattacks.[3] Regardless, a broad cross section of groups agreed that the FCC should provide guidance.[4] But instead of doing so, either in response to that petition or otherwise, Commission leadership made it abundantly clear that such guidance would not be forthcoming,[5] and the agency ultimately dismissed the petition.[6]

[1] *See* Petition for Declaratory Ruling or, in the Alternative, for Rulemaking, RM-11737 (Aug. 25, 2014), *available at* http://go.usa.gov/ccjxT.

[2] *See, e.g.*, Google Opposition, RM-11737, at 1 (Dec. 19, 2014) ("[W]hile Google recognizes the importance of leaving operators flexibility to manage *their own* networks, this does not include intentionally blocking access to other Commission-authorized networks."); *see also* National Cable and Telecommunications Association Opposition, RM-11737 (Dec. 19, 2014).

[3] *See, e.g.*, USTelecom Comments, RM-11737, at 2 (Dec. 22, 2014) ("[T]he Commission at the very least should clarify that a Wi-Fi operator does not violate the statute when mitigating network threats."); *see also* Cisco Comments, RM-11737, at 2 (Dec. 19, 2014) ("[A]ccess to unlicensed spectrum resources can and should be balanced against the need to protect networks, data and devices from security threats and potentially other limited network management concerns.").

[4] *See, e.g.*, Enterprise Wireless Alliance Comments, RM-11737, at 1–2 ("EWA urges the Commission to undertake a rulemaking and adopt rules that clarify this important issue for the benefit of Wi-Fi network operators and consumers."); Ad Hoc Telecommunications Users Committee Statement, RM-11737, at 2 (Dec. 19, 2014) ("Ad Hoc supports the initiation of a rulemaking in order for the Commission to develop a robust factual record on the basis of which it can then establish clear, generally applicable standards and policies."); Letter from Harold Feld, Public Knowledge, to Marlene H. Dortch, FCC, RM-11737 (Feb. 13, 2015) ("Where the largest hotel chains, the largest trade associations of network operators, and numerous equipment manufacturers come to different conclusions as to the applicability of Section 333, it is clear that a controversy exists requiring the Commission to issue a definitive statement of policy.").

[5] *See* Remarks of FCC Commissioner Jessica Rosenworcel, State of the Net Conference (Jan. 27, 2015) (calling on the Commission "to dismiss this petition without delay"), *available at* http://go.usa.gov/ca5PP; *see also* FCC Chairman Tom Wheeler Statement on Protecting Consumers from Hotel Wi-Fi Blocking (Jan. 27, 2015), *available at* http://go.usa.gov/ca5mT.

[6] *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*, RM-11737, Order, 30 FCC Rcd 1251 (Wireless Telecomm. Bur. 2015).

Flash forward to today. In this case, the Commission proposes to fine a company $718,000 for engaging in Wi-Fi blocking. But here's the rub. Because the Commission dropped the ball earlier this year, we do not have any rules that limit Wi-Fi blocking. Indeed, the only relevant rules we have on the books preclude liability in these circumstances.

To be sure, the *Notice of Apparent Liability* (*NAL*) takes a contrary position. It asserts that the Commission did not need to adopt or modify any rules because of section 333 of the Communications Act. That section states that "[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications," and the agency argues that it has always prohibited the operator of an unlicensed Part 15 device from intentionally disrupting the operation of another unlicensed Part 15 device.[7] But the Commission's attempt to apply section 333 to interference between Part 15 devices fails as a matter of law.

*First*, by definition, a Part 15 device cannot cause harmful interference to another Part 15 device.[8] Under the agency's rules, a Part 15 device can cause harmful interference to a device operating in a licensed service, such as in a cellular band, and such interference is prohibited.[9] But because of the shared, "commons" model that applies to all unlicensed operations, the Commission has repeatedly held that "interference caused to a Part 15 device by another Part 15 device does not constitute harmful interference."[10] Whether that *should* be the law is a question worth exploring, as I've noted above. But it *is* the law now. That fact is fatal to the *NAL*'s attempt to apply section 333 to unlicensed operations because it means that the Commission is proposing to fine a company for doing something that the FCC says carries no legal liability—namely, operating a Part 15 device in a manner that intentionally disrupts the operation of another Part 15 device.[11]

*Second*, and relatedly, section 333 does not apply because the FCC's Part 15 rules provide that unlicensed devices must accept any and all interference they receive, regardless of the source of that interference.[12] As the Commission has determined, "[i]t does not matter who operates the unlicensed

---

[7] Communications Act § 333.

[8] *See, e.g.*, *Remington Arms Company, Inc. Request for a Waiver of the Part 15 Regulations*, ET Docket No. 05-183, Order, 20 FCC Rcd 18724, 18727 n.12 (2005) (*Remington Order*) (stating that "the requirement to resolve harmful interference caused to other users does not apply to . . . other users of Part 15 transmission systems" because "Part 15 is not a radio service"); *Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems*, ET Docket No. 98-153, Order, 17 FCC Rcd 13522, 13524 n.7 (Office of Engineering & Technology 2002) (*Ultra-Wideband Order*) ("Harmful interference consists of interference to a radiocommunications service. *See* 47 C.F.R. § 15.3(m). Part 15 devices are not part of a 'service.' Thus, interference caused to a Part 15 device by another Part 15 device does not constitute harmful interference.").

[9] *See* 47 C.F.R. § 15.5(b); *see also* 47 C.F.R. § 15.3(m).

[10] *Remington Order*, 20 FCC Rcd at 18727 n.12; *Ultra-Wideband Order*, 17 FCC Rcd at 13524 n.7; *see also Allocations and Service Rules for the 71–76 GHz, 81–86 GHz and 92–95 GHz Bands; Loea Communications Corporation Petition for Rulemaking*, WT Docket No. 02-146, RM-10288, Report and Order, 18 FCC Rcd 23318, 23346, n.185 (2003) ("The 'commons' model allows unlimited numbers of unlicensed users to share frequencies, with usage rights that are governed by technical standards or etiquettes but with no right to protection from interference.").

[11] The fact that section 333 prohibits a person from "willfully or maliciously interfer[ing]," whereas the FCC's Part 15 rules provide that unlicensed devices are excluded from the definition of "harmful interference," does not aid the Commission's case. Since there is no liability for causing harmful interference, there can be no liability for willfully or maliciously causing mere interference.

[12] *See* 47 C.F.R. § 15.5(b) ("Operation . . . is subject to the condition[] . . . that interference must be accepted[.]"); *see also Remington Order*, 20 FCC Rcd at 18727, para. 10 ("[A]ll Part 15 devices, including WiFi systems, LANs, and meter reading systems, operate on a sufferance basis where the operator is required to accept any interference that is received, regardless of the source of that interference.").

equipment or the purpose for which the equipment is used—no protection against received interference is provided or available."[13] Thus, as Cisco has explained, "[i]t simply cannot be that a Part 15 device is both unprotected against interference under Section 15.5(b) [of the Commission's rules] but protected against interference under Section 333" of the Communications Act.[14]

So how does the *NAL* reconcile its newfound take on section 333 with these longstanding Commission rules and precedents? It doesn't. It simply recites the part of section 333 that says "[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications" and asserts that, *a fortiori*, the provision prohibits a Part 15 device from interfering with another Part 15 device. But what about the FCC's decision to define harmful interference in a way that excludes Part 15 devices? What about the agency's decision to require Part 15 devices to accept any and all interference? These still-binding rules and precedents are ignored entirely.

Moreover, attempting to apply section 333 to unlicensed operations is not just contrary to law, it produces absurd and illogical results. Think about it. By the very nature of their shared use of spectrum, unlicensed devices routinely interfere with each other. When someone at a coffee shop uses Wi-Fi to surf the Internet or someone else relies on a Bluetooth connection to play music over a wireless speaker, they may very well be interrupting or causing harmful interference to another unlicensed device. Does anyone seriously believe that these routine uses of unlicensed technology violate section 333? I would hope not.

Yet that is exactly the result that the *NAL*'s reading of section 333 compels. The provision prohibits any person from "willfully" interfering with covered communications.[15] And recall that both the Communications Act and the FCC define "willful" as the conscious decision to act, irrespective of a person's motivation or intent to violate the law.[16] So if section 333 applies to unlicensed operations, then that necessarily means that every time a consumer uses Wi-Fi, Bluetooth, or any other unlicensed technology, the FCC could find that they have willfully interfered with another unlicensed device in violation of federal law and thus subject them to millions of dollars in fines. It would make no difference that the consumer did not intend to disrupt lawful communications. This absurd outcome illustrates why the FCC has never read section 333 as applying to interference between unlicensed devices.

At the very least, all of this underscores a final reason why the Commission cannot lawfully apply section 333 in this case—it has failed to comport with due process. As explained above, I believe it is clear that Wi-Fi blocking is currently lawful under the Commission's rules. But even if I am wrong about that, the Commission's case would still founder. That is because it is certainly not clear that Wi-Fi blocking is currently unlawful under the Commission's rules. And a core principle of the American legal system is that the government cannot sanction you for violating the law unless it has told you what the law is.[17] In the regulatory context, due process is protected, in part, through the fair warning rule.

---

[13] *Remington Order*, 20 FCC Rcd at 18727, para. 10.

[14] Cisco Comments, RM-11737, at 18 (Dec. 19, 2014).

[15] Communications Act § 333.

[16] *See* Communications Act § 312(f)(1) ("The term 'willful', when used with reference to the commission or omission of any act, means the conscious and deliberate commission or omission of such act, irrespective of any intent to violate any provision of this chapter or any rule or regulation of the Commission authorized by this chapter or by a treaty ratified by the United States."); *see also Playa Del Sol Broadcasters; Licensee of Station K238AK Palm Desert, California*, File No. EB-08-SD-0088, Order on Review, 28 FCC Rcd 2666, 2667–68, para. 4 (2013) (stating that the Commission interprets the term "willful," as it is used in section 503 of the Communications Act, as "the 'conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate' the law" (quoting Communications Act § 312(f)(1)).

[17] *See, e.g.*, *Mullane v. Central Hanover Tr. Co.*, 336 U.S. 306, 313 (1950); *see also TerraCom, Inc. and YourTel America, Inc.*, File No. EB-TCD-13-00009175, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13349 n.1 (2014) (Dissenting Statement of Commissioner Ajit Pai) (collecting authorities).

Specifically, the D.C. Circuit has stated that "[i]n the absence of notice—for example, where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property."[18] Thus, an agency cannot at once invent and enforce a legal obligation.

Yet that is precisely what has happened here. Prior to this *NAL*, the Commission never interpreted section 333 as prohibiting interference between unlicensed devices.[19] The 2011 and 2012 Bureau-level Enforcement Advisories to which the *NAL* points certainly didn't.[20] They simply reminded consumers that they cannot use jammers—which are not Part 15 devices and have no lawful application—regardless of whether those jammers interfere with a licensed service or Wi-Fi communications. They have nothing to do with interference *between* Part 15 devices and whether such interference constitutes a violation of section 333. Nor could they, given the full Commission's determination that Part 15 devices cannot cause harmful interference, as discussed above.

Nor is the *NAL* right to rely on two Bureau-level consent decrees to satisfy the fair-warning rule. By their very terms, those documents state that they "do[] not constitute either an adjudication on the merits or a factual or legal finding or determination regarding any compliance or noncompliance with the Communications Law."[21]

* * *

There is widespread agreement that we should take action to limit Wi-Fi blocking. The disagreement is over how we should go about doing that. I believe that we should adopt rules that clearly set forth when Wi-Fi blocking is unlawful and when, if ever, it is lawful. And I stand ready to work with my colleagues to craft such rules and then enforce them. But I cannot support taking enforcement action against a party that has not violated any statutory provision or Commission rule.

In the end, this decision is the latest evidence that the FCC's enforcement process has gone off the rails. Instead of dispensing justice by applying the law to the facts, the Commission is yet again

---

[18] *General Electric Co. v. U.S. Environmental Protection Agency*, 53 F.3d 1324, 1328 (D.C. Cir. 1995); *see also United States v. Chrysler*, 158 F.3d 1350, 1354–55 (D.C. Cir. 1998) (discussing the "well-established rule in administrative law that the application of a rule may be successfully challenged if it does not give fair warning that the allegedly violative conduct was prohibited").

[19] *See, e.g.*, *R&N Manufacturing, Ltd. Houston, Texas*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 3332 (2014) (proposing fine for causing interference to cellular and PCS communications).

[20] *Cell Jammers, GPS Jammers, and Other Jamming Devices; Consumers Beware: It is Unlawful to Use "Cell Jammers" and Other Equipment that Blocks, Jams, or Interferes with Authorized Radio Communications in the U.S.*, Public Notice, 26 FCC Rcd 1329 (Enf. Bur. 2011); *Cell Jammers, GPS Jammers, and Other Jamming Devices; Consumer Alert: Using or Importing Jammers is Illegal*, Public Notice, 27 FCC Rcd 2309 (Enf. Bur. 2012).

[21] *Marriott Int'l, Inc., Marriott Hotel Services, Inc.*, File No.: EB-IHD-13-00011303, Order and Consent Decree, 29 FCC Rcd 11760, 11768 (Enf. Bur. 2014); *Smart City Holdings, LLC and its Wholly-Owned Subsidiaries, Smart City Networks, LP, and Smart City Solutions, LLC*, File No.: EB-SED-15-00018248, Order and Consent Decree, 30 FCC Rcd 8382, 8390 (Enf. Bur. 2015). Likewise, the *NAL*'s statement that *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015), held that consent decrees provided fair warning misses the mark. *See NAL* at para. 33, n.101. Among other things, *Wyndham* held no such thing. Rather, the Third Circuit stated: "We agree with Wyndham that the consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by" the applicable statute. *Wyndham*, 799 F.3d at 257 n.22. So too here. In fact, the most the *NAL* actually says about the Marriott and Smart City consent decrees is that they show that the Commission "could consider" Wi-Fi blocking a violation of section 333. *See NAL* at para. 33. But that's not the test. Again, the *NAL* appears to be relying on *Wyndham* for this "could consider" language, but in doing so it ignores that *Wyndham* did not involve the fair warning rule at all. It involved a different test that applies when a court—not an agency—is called upon to interpret a statute in the first instance. *See, e.g.*, *Wyndham*, 799 F.3d at 253 ("[T]his case involves ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply.").

focused on issuing headline-grabbing fines. And while I have no doubt that this *NAL* will generate plenty of press, I cannot support this lawless item. Therefore, I respectfully dissent.

**DISSENTING STATEMENT OF COMMISSIONER MICHAEL O'RIELLY**

Re: *M.C. Dean, Inc., File No.: EB-SED-15-00018428, NAL/Acct. No.: 201532100008, FRN: 0011134921, Notice of Apparent Liability for Forfeiture*

A little over a year ago, I became aware of the contention that the use of deauthentification technology to manage Wi-Fi systems violates section 333 of the Communications Act.[1] I respectfully requested that the Commission undertake a rulemaking or other proceeding to consider this issue more thoroughly, instead of pursuing an enforcement action. This seemed like a reasonable request when there was already a petition – and corresponding comments – on file. Alas, my request was rejected and the petition eventually withdrawn (conveniently after some of the petitioners entered into a consent decree with the Enforcement Bureau),[2] leaving the substantive concerns unaddressed. So that brings us to another suspect enforcement item without the underlying work being done.

As a strong supporter of what Wi-Fi can bring to consumers and the marketplace, I am extremely sympathetic to concerns regarding certain operators needlessly interfering with access points. I, however, cannot agree with the expansive reading of the statute contained in this item, especially without the Commission conducting a more thorough review of the issues raised in the earlier proceeding and repeated in the context of this enforcement matter.

Section 333 prohibits willful or malicious interference "to any radio communication of any station licensed or authorized by or under this Act."[3] There is no clear intent that Congress meant to ensnare Part 15 devices when it used the word "station." The legislative history highlights several services and contains language that indicate that Congress meant to protect stations that are licensed or licensed by rule, as opposed to unlicensed spectrum or devices, which are never mentioned, even though Part 15 was in existence decades before section 333 was adopted.[4]

There are legitimate concerns that equating Part 15 devices to "stations" appears inconsistent with prior Commission actions and could have serious regulatory repercussions for unlicensed users. For instance, if such devices are "stations," would they be subject to other licensing provisions of the Act,[5] such as foreign ownership restrictions and transfer of control provisions,[6] among others? The

[1] 47 U.S.C. § 333.

[2] *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*, RM-11737, Order, 10 FCC Rcd 1251 (WTB 2015).

[3] 47 U.S.C. § 333.

[4] Congress noted that there was an increase in interference instances to certain radio services that warranted a statutory solution, because the authority that was being used under "the more limited licensed operator provision of the Act" only allowed for remedy after lengthy and complex administrative proceedings. The services highlighted were amateur, maritime, citizens band radio, public safety, private land mobile and cable television. The legislative history states that the provision "prohibits intentional jamming, deliberate transmissions on top of the transmission of authorized operators already using specific frequencies in order to obstruct their communication, repeated interruptions, and the use and transmission of whistles, tapes, records, or other types of noisemaking devices to interfere with the communications or radio signals of other stations." H.R. Rep. 101-316, at 8 (Oct. 27, 1989); *see also* S. Rep. 101-215, at 7 (Nov. 19, 1989).

[5] 47 U.S.C. § 307.

[6] *Id.* § 310.

Commission has never applied these sections to Wi-Fi operators. In fact, devices and stations traditionally have been treated differently under both the statute and Commission rules.[7]

Some have also raised whether the use of deauthentification frames constitutes interference under section 333. For example, the Commission's definition of interference is "[t]he effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy."[8] It appears that this provision applies to mechanisms that intentionally cause electromagnetic interference, such as jammers, and not to deauthentification frames, which do not increase the level of energy overpowering communications signals in an area.

There is also a debate regarding potential inconsistencies between section 333 and the Part 15 rules. Under section 15.5(b) of the Commission's rules, unlicensed devices can cause interference to and must accept interference from other Part 15 devices.[9] On the other hand, if section 333 applies to a Part 15 device, such a device would be prohibited from "willfully and maliciously interfer[ing] with or caus[ing] interference to" other unlicensed devices. This language appears to directly contravene the language of section 15.5(b). If applied, the statutory language of section 333, as written, could undermine the regulatory structure of unlicensed operations and potentially subject all Wi-Fi users to potential enforcement action whenever they "willfully" operate Wi-Fi equipment.[10]

Despite these valid concerns, we are, once again, trying to set important and complex regulatory policy by enforcement adjudication. This is backward and not the best course of action. Besides this Notice of Apparent Liability, the Commission has never considered whether using deauthentification software violates the statute or Commission policy. The Enforcement Bureau – not the Commission – has issued two consent decrees[11] and four enforcement advisories, three of which are actually about

[7] For example, the Commission's rules pertaining to unlicensed use clearly differentiates between "an authorized radio station" and intentional, unintentional or incidental radiators, which are devices. 47 C.F.R. § 15.5(b). Additionally, Section 302 of the Communications Act, 47 U.S.C. § 302(a), allows the Commission to "make reasonable regulations . . . governing the interference potential of devices which in their operation are capable of emitting radio frequency energy…." At no point is there any reference to these devices being stations. Section 706(c) of the Communications Act, 47 U.S.C. § 606, delineating the powers of the President in a war or emergency also differentiates between stations and devices. Section 2.939(b) of the Commission's rules also differentiates between station and devices when it states that "[r]evocation of an equipment authorization shall be made in the same manner as revocation of radio station licenses." 47 C.F.R. § 2.939(b).

[8] 47 C.F.R. § 2.1.

[9] Section 15.5(b) states that the "operation of an intentional, unintentional, or incidental radiator is subject to the conditions that no harmful interference is caused and that interference must be accepted that may be caused by the operations of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator." 47 C.F.R. § 15.5(b).

[10] 47 U.S.C. § 312(f)(1) ("The term 'willful', when used with reference to the commission or omission of any act, means the conscious and deliberate commission or omission of such act, irrespective of any intent to violate any provision of this chapter or any rule or regulation of the Commission authorized by this chapter or by a treaty ratified by the United States.").

[11] *Marriott International, Inc., Marriott Hotel Services, Inc.*, File No.: EB-IHD-13-00011303, Acct. No.: 201532080001, FRN: 0006183511, Order, 29 FCC Rcd 11760 (EB 2014); *Smart City Holdings, LLC, and its Wholly-Owned Subsidiaries, Smart City Networks, LP, and Smart City Solutions LLC*, File No.: EB-SED-15-00018248, Acct. No.: 201532100006, FRN: 0024681223, Order, 30 FCC Rcd 8382 (EB 2015).

jammers.[12] Enforcement advisories and consent decrees do not serve as Commission precedent. Moreover, the last advisory, which the Enforcement Bureau must have found necessary due the unclear regulatory state, was released *after* the suspected behavior in this case.[13] Even if one accepts the belief that such advisories are worth something, how is that sufficient notice or fair?

The simple, which happens to correspond to the appropriate, solution to this controversy, is to either seek Congressional clarification or conduct a broad rulemaking on the potential reach of section 333 to Part 15 devices. That way all views can be explored by the Commission and objectors would have a remedy process via the court system.

As a side note, this item, yet again, fails to state with particularity how the Commission calculated the upward adjustment. I continue to be unable to support upward adjustments that are meant to penalize entities for potential violations *outside* of the statute of limitations period.

For the reasons stated above, I dissent.

[12] *FCC Enforcement Advisory; Warning: Jammer Use is Prohibited*, Enforcement Advisory No. 2014-05, Public Notice, 29 FCC Rcd 14737 (EB 2014); *FCC Enforcement Advisory; Cell Jammers, GPS Jammers, and Other Jamming Devices; Consumer Alert: Using or Importing Jammers is Illegal*, Enforcement Advisory No. 2012-02, Public Notice, 27 FCC Rcd 2309 (EB 2012); *FCC Enforcement Advisory; Cell Jammers, GPS Jammers, and Other Jamming Devices; Consumers Beware: It is Unlawful to Use "Cell Jammers" and Other Equipment that Blocks, Jams, or Interferes with Authorized Radio Communications in the U.S.*, Enforcement Advisory No. 2011-04, Public Notice, 26 FCC Rcd 13299 (EB 2011).

[13] *FCC Enforcement Advisory; Warning: Wi-Fi Blocking is Prohibited*, Enforcement Advisory No. 2015-01, Public Notice, 30 FCC Rcd 387 (EB 2015).