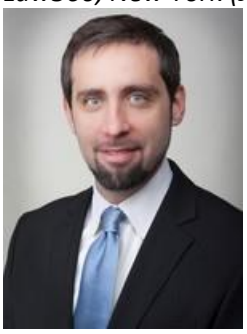
Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FCC Keeps Blocking Hospitality Wi-Fi Blocking

Law360, New York (January 19, 2016, 12:19 PM ET) --


Abraham J. Rein


Charles W. Spitz

Late last year, the U.S. Federal Communications Commission took another enforcement step in its aggressive, ongoing campaign against Wi-Fi blocking — the practice of blocking unauthorized Wi-Fi hotspots that let consumers share mobile data access with other devices, like laptops and tablets — in hotels and convention spaces. It released a Notice of Apparent Liability for Forfeiture (NALF) indicating that it will issue a $718,000 fine against M.C. Dean Inc. in connection with Wi-Fi blocking at the Baltimore Convention Center (BCC). M.C. Dean is fighting the fine, in the first such challenge to the Commission's authority to police business premises wireless network management.

The M.C. Dean NALF

In the M.C. Dean NALF, the FCC accused M.C. Dean — the contractor that provides telecommunications and internet services to the BCC — of operating its network management system in what the system's user manual called "'shoot first and ask questions later' mode" for approximately two years, between October 2012 and December 2014. According to the FCC, that setting allowed M.C. Dean's hardware to routinely and repeatedly disrupt links between wireless devices in use at the BCC and any Wi-Fi network other than M.C. Dean's. Through the use of this feature, the FCC alleged, M.C. Dean "automatically detected and indiscriminately deauthenticated any unknown [point of wireless access to the internet]." The alleged result was that many visitors found their personal Wi-Fi hotspots unusable at the convention center.

The NALF implied that M.C. Dean's motive in disrupting unknown wireless networks operating in the BCC was to force visitors to purchase wireless service from M.C. Dean itself. (For its part, M.C. Dean — like other operators of large wireless networks in the hospitality industry — advances various practical justifications for these sorts of network management practices —more on this below.) The FCC concluded that Wi-Fi blocking activity represents "a particularly egregious form of misconduct," which

“runs counter to fundamental Commission principles by stymieing wireless innovation, competition and the availability of Wi-Fi as an important Internet access technology.” Because the FCC deemed the conduct especially offensive, and “to ensure that a proposed forfeiture is not treated as simply a cost of doing business,” the FCC proposed a fine of $718,000 — just shy of *four times* the base figure suggested by the Commission’s forfeiture guidelines.

M.C. Dean has declined to accept the FCC’s proposed forfeiture, making a submission that describes the Commission’s legal theory as “akin to a second-rate B-movie Dracula that collapses when exposed to the realities of daylight” and urging that the NALF be “dispatched with the regulatory equivalent of a wooden stake through the heart: a summary cancelation or withdrawal.” M.C. Dean argues that, not only is the FCC wrong about its motives — the vast majority of its wireless service sales take place prior to the events and so revenues are not boosted by any real-time blocking activity — the enforcement action amounts to an unfair surprise. The FCC, argues M.C. Dean, itself authorized the equipment that the company used, with the result that “the company reasonably believed that such authorization extended to the [equipment’s] deauthentication technology”; not only that, but the FCC’s legal theory is novel and M.C. Dean claims it had no notice that the conduct might violate the FCC’s rules.

Ongoing Battle

The FCC has made its anti-Wi-Fi blocking efforts into something of a campaign. Simultaneously with issuing the M.C. Dean NALF, the FCC issued a separate NALF indicating it will issue a $25,000 fine against Hilton Hotels for a failure to cooperate in the FCC’s investigation of Wi-Fi blocking at Hilton properties around the world. The Hilton and M.C. Dean actions came on the heels of a $750,000 settlement with Smart City Holdings over its Wi-Fi blocking at multiple convention centers, and a late-2014 settlement of $600,000 with Marriott over similar conduct.

In the wake of the Marriott settlement, industry groups petitioned the Commission for a declaration or rulemaking clarifying the FCC’s stance toward certain sophisticated Wi-Fi management techniques, which can be valuable tools for protecting consumers on business premises, and for protecting the businesses themselves. The FCC aggressively rebuffed the petition, issuing multiple statements on Jan. 27, 2015 to the effect that the FCC does not countenance Wi-Fi blocking, period. The industry groups, faced with a near-certain public flogging, withdrew their petition. They had little choice, but the move meant that important and complex questions regarding Wi-Fi network management on hotel and other business premises would remain unanswered.

In the course of withdrawing the petition, the American Hotel & Lodging Association highlighted the legitimate security concerns associated with unchecked hotspot use in a physical space crowded with Wi-Fi users, telling the FCC:

Broad access to Wi-Fi is among the capabilities that petitioners' guests demand. They also demand access to a safe and secure system in order to protect private information from criminals seeking to exploit consumers. ... Of particular concern to the hospitality industry is the ability of a hotel to protect the security of its network and guests by using wireless intrusion detection and prevention systems that are part of WLAN equipment authorized by the FCC. These systems are employed by numerous WLAN operators across multiple industries, including the federal government.

The M.C. Dean NALF appears to signal again the FCC’s blunt rejection of the industry group’s concerns.

Legitimate Concerns

The FCC's rejection notwithstanding, there are important considerations at play. Depending on how strictly the FCC interprets its perceived anti-blocking powers, for example, hotels and convention centers could well be deprived of an effective tool for protecting patrons against dangerous and widespread scams. In one such scam, a would-be cyberthief sets up a Wi-Fi hotspot that acts as an "evil twin" to the business's legitimate network, giving the bogus wireless network the same name and characteristics as the business's. When unsuspecting visitors use the illegitimate wireless, the bad actor can often collect the data that passes across his equipment, exposing private information such as usernames, passwords, credit card information and private messages. Deprived of the ability to disrupt the connection between an evil twin and its putative victims — because the FCC has described the "use of deauthentication frames with the intent to prevent third-party Wi-Fi devices from establishing or maintaining their own networks" as a violation — businesses may be without their most powerful tool for protecting their customers against such misdeeds.

Another concern is performance. Particularly in the hospitality industry, where customers are often businesspeople who expect and require on-premises connectivity to do their jobs, reliable Wi-Fi is a necessity, not a luxury. But when a relatively small physical space is packed with a large number of individual wireless hotspots, some of them operating at a much higher power than others, those devices can interfere with one another and network performance, including the performance of the business's network, can suffer. Businesses may be prevented from policing their airspace to avoid significant interference from particularly disruptive devices. The fact that resulting on-premises connectivity problems may be perceived by customers as unlawful Wi-Fi blocking, contrary to the FCC's recent enforcement actions, is an irony that businesses may have to endure.

Controversy Within the Commission

Commissioners Michael O'Rielly and Ajit Pai dissented from the M.C. Dean NALF, echoing the industry's unease over the FCC's aggressive enforcement absent clear rules. Both commissioners questioned whether the current state of the law even allows the FCC to prohibit the type of Wi-Fi management at issue, noting that the Commission's interpretation of the law could lead to absurd results, including that — because, as noted above, Wi-Fi signals in close proximity to one another clash — every intentional use of wireless equipment in a public space could invite sanctions.

Commissioner Pai called the decision "the latest evidence that the FCC's enforcement process has gone off the rails," accusing the Commission of "yet again focus[ing] on attention-grabbing fines," "instead of dispensing justice by applying the law to the facts." A month later, he echoed those comments at an event for communications attorneys, saying that "things have gone seriously awry" in the Commission's enforcement process and chastising the FCC Enforcement Bureau for neglecting the unglamorous, meat-and-potatoes enforcement that has traditionally been its beat in favor of eye-popping fines that attract press but do not necessarily further the Commission's mission.

Commissioner Pai's concerns are apparently shared by some at the federal government's other top cyber enforcer, the Federal Trade Commission. The day after Commissioner Pai's remarks, FTC Commissioner Maureen Ohlhausen gave a speech ("FTC-FCC: When Is Two a Crowd?") to the same audience that contrasted the FCC's and FTC's enforcement priorities and noted:

The FCC's approach ... differs significantly from the FTC's "reasonable security" approach. I am concerned that what appears to be a "strict liability" data security standard will actually harm

consumers. The goal of consumer protection enforcement isn't to make headlines; it is to make harmed consumers whole and incentivize appropriate practices.

Commissioner O'Rielly said that the M.C. Dean NALF illustrates the poor fit between legislation and regulation developed in a pre-Wi-Fi world and the problems of the present day. He called the enforcement an example of, "yet again, trying to set important and complex regulatory policy by enforcement adjudication," adding, "[t]his is backward and not the best course of action."

Conclusion

The FCC appears set on aggressively moving against Wi-Fi blocking without answering crucial questions about which available network management techniques are FCC-approved. This state of affairs is increasingly common in issues of cybersecurity, where slow-moving regulators meet fast-developing technology. The FCC has made it clear that it will look with a jaundiced eye on practices that fail to meet its expectations; what exactly those expectations are appears destined to be developed piecemeal, one enforcement action at a time.

—By Abraham J. Rein and Charles W. Spitz, Post & Schell PC

Abraham Rein is an associate in Post & Schell's Philadelphia office and was part of the team that won the Facebook speech case, United States v. Elonis, in the Supreme Court of the United States.

Charles Spitz is principal and chairman of Post & Schell's hospitality practice group and is based in Philadelphia.