



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

June 29, 2015

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Johnson:

Thank you for your letter concerning the Federal Communications Commission's position on the use of Wireless Intrusion Detection Systems and Wireless Intrusion Prevention Systems (WIDS/WIPS) to protect wireless networks and users from cyberattacks. Your letter raises important legal and policy questions that underscore the need to balance the practical needs of network operators to protect their systems with consumers' expectation of easy utilization of Wi-Fi access points. The FCC is committed to striking the right balance between ready access to unlicensed spectrum and effective cyber defense. Accordingly, our enforcement activity in this arena has focused on circumstances where companies are not "defending" their networks, but instead are using these capabilities to knowingly deny legitimate users access to shared unlicensed spectrum.

Your letter expresses concern regarding a perceived tension between the FCC Enforcement Bureau's January 27, 2015 Enforcement Advisory on Wi-Fi blocking,¹ and the Department of Homeland Security's *Wireless Local Area Network (WLAN) Reference Architecture* publication regarding the use of WIDS/WIPS by Federal agencies.² Although the Commission's jurisdiction is limited to non-federal uses of the radiofrequency spectrum, we understand the two documents to be consistent in their positions that network operators should not use "blocking" to interfere with the operation of independent wireless networks.

As a general matter, Enforcement Advisories serve to educate businesses and consumers about what the Communications Act of 1934, as amended, and the FCC's rules require, the purpose and importance of those laws and rules, and the consequences of failure to comply. Enforcement Advisories thus simply illuminate issues for the benefit of the public and entities that may be subject to the Commission's jurisdiction.

¹ See https://apps.fcc.gov/edocs_public/attachmatch/DA-15-113A1.pdf ("FCC ENFORCEMENT ADVISORY—WARNING: Wi-Fi Blocking is Prohibited"). Your letter also references an Enforcement Advisory issued on March 6, 2012. See https://apps.fcc.gov/edocs_public/attachmatch/DA-12-347A1.pdf ("FCC CONSUMER ALERT: Using or Importing Jammers is Illegal").

² Dep't of Homeland Sec., Nat'l Cyber Sec. Div., *Wireless Local Area Network (WLAN) Reference Architecture* sect. 4.4 (2011) (DHS Reference Architecture).

The Enforcement Advisory referenced in your letter provided narrowly tailored guidance regarding behavior that is prohibited by Section 333 of the Communications Act, which states that “[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this Act or operated by the United States Government.” The Enforcement Advisory did not change policy regarding the legitimate use of WIDS/WIPS by non-federal users and does not address any practices of federal government network operators, over which the FCC has no statutory jurisdiction.

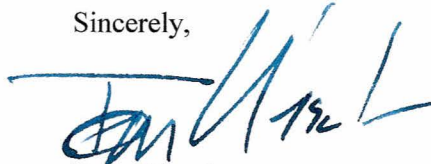
The Enforcement Advisory states that no hotel, convention center, or other commercial establishment or the network operator providing services at such establishments, may intentionally block or disrupt personal Wi-Fi hot spots on such premises, including as part of an effort to force consumers to purchase access to the property owner's Wi-Fi network. The Enforcement Bureau issued this advisory following its 2014 Consent Decree with Marriott International, Inc., in which the company deployed a Wi-Fi deauthentication protocol to deliberately and indiscriminately block consumers who sought to connect to the Internet using their own personal Wi-Fi hot spots. In that case, Marriott admitted that the customers it blocked did not pose a security threat to the Marriott network and agreed to settle the investigation. Because the FCC had received several complaints that other commercial Wi-Fi network operators might be disrupting the legitimate operation of personal Wi-Fi hot spots, the Enforcement Bureau issued the advisory to provide more information to businesses and consumers.

The Enforcement Advisory is consistent with the DHS document. For example, the DHS document states that a federal agency should recognize that there may be independent Wi-Fi networks in the vicinity of the agency's operations and the agency should not configure its WIDS/WIPS to automatically block them. Indeed, the DHS document calls for federal agencies to address and plan for legitimate external Wi-Fi use, and notes that WIDS/WIPS have features that enable a security specialist to monitor legitimate threats while identifying non-threats caused by these cases of overlapping local area networks.

The FCC recognizes and values the significant experience that DHS and other federal partners bring to this crucial cybersecurity discussion, and the FCC and DHS regularly share expertise in support of our independent yet complementary missions. The FCC enjoys a longstanding and mutually-beneficial working relationship with DHS and other interagency partners.

Thank you for your interest in this matter. The security of our nation's communications network is vital to both private and public sectors. We recognize that there is additional work to do to define defensible best practices for shared unlicensed bands, and we look forward to working with our federal partners to develop these best practices.

Sincerely,



Tom Wheeler



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

June 29, 2015

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, D.C. 20515

Dear Chairman McCaul:

Thank you for your letter concerning the Federal Communications Commission's position on the use of Wireless Intrusion Detection Systems and Wireless Intrusion Prevention Systems (WIDS/WIPS) to protect wireless networks and users from cyberattacks. Your letter raises important legal and policy questions that underscore the need to balance the practical needs of network operators to protect their systems with consumers' expectation of easy utilization of Wi-Fi access points. The FCC is committed to striking the right balance between ready access to unlicensed spectrum and effective cyber defense. Accordingly, our enforcement activity in this arena has focused on circumstances where companies are not "defending" their networks, but instead are using these capabilities to knowingly deny legitimate users access to shared unlicensed spectrum.

Your letter expresses concern regarding a perceived tension between the FCC Enforcement Bureau's January 27, 2015 Enforcement Advisory on Wi-Fi blocking,¹ and the Department of Homeland Security's *Wireless Local Area Network (WLAN) Reference Architecture* publication regarding the use of WIDS/WIPS by Federal agencies.² Although the Commission's jurisdiction is limited to non-federal uses of the radiofrequency spectrum, we understand the two documents to be consistent in their positions that network operators should not use "blocking" to interfere with the operation of independent wireless networks.

As a general matter, Enforcement Advisories serve to educate businesses and consumers about what the Communications Act of 1934, as amended, and the FCC's rules require, the purpose and importance of those laws and rules, and the consequences of failure to comply. Enforcement Advisories thus simply illuminate issues for the benefit of the public and entities that may be subject to the Commission's jurisdiction.

¹ See https://apps.fcc.gov/edocs_public/attachmatch/DA-15-113A1.pdf ("FCC ENFORCEMENT ADVISORY—WARNING: Wi-Fi Blocking is Prohibited"). Your letter also references an Enforcement Advisory issued on March 6, 2012. See https://apps.fcc.gov/edocs_public/attachmatch/DA-12-347A1.pdf ("FCC CONSUMER ALERT: Using or Importing Jammers is Illegal").

² Dep't of Homeland Sec., Nat'l Cyber Sec. Div., *Wireless Local Area Network (WLAN) Reference Architecture* sect. 4.4 (2011) (DHS Reference Architecture).

The Enforcement Advisory referenced in your letter provided narrowly tailored guidance regarding behavior that is prohibited by Section 333 of the Communications Act, which states that “[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this Act or operated by the United States Government.” The Enforcement Advisory did not change policy regarding the legitimate use of WIDS/WIPS by non-federal users and does not address any practices of federal government network operators, over which the FCC has no statutory jurisdiction.

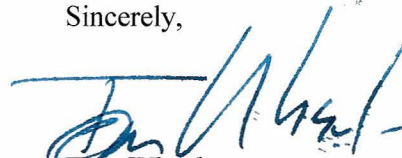
The Enforcement Advisory states that no hotel, convention center, or other commercial establishment or the network operator providing services at such establishments, may intentionally block or disrupt personal Wi-Fi hot spots on such premises, including as part of an effort to force consumers to purchase access to the property owner's Wi-Fi network. The Enforcement Bureau issued this advisory following its 2014 Consent Decree with Marriott International, Inc., in which the company deployed a Wi-Fi deauthentication protocol to deliberately and indiscriminately block consumers who sought to connect to the Internet using their own personal Wi-Fi hot spots. In that case, Marriott admitted that the customers it blocked did not pose a security threat to the Marriott network and agreed to settle the investigation. Because the FCC had received several complaints that other commercial Wi-Fi network operators might be disrupting the legitimate operation of personal Wi-Fi hot spots, the Enforcement Bureau issued the advisory to provide more information to businesses and consumers.

The Enforcement Advisory is consistent with the DHS document. For example, the DHS document states that a federal agency should recognize that there may be independent Wi-Fi networks in the vicinity of the agency's operations and the agency should not configure its WIDS/WIPS to automatically block them. Indeed, the DHS document calls for federal agencies to address and plan for legitimate external Wi-Fi use, and notes that WIDS/WIPS have features that enable a security specialist to monitor legitimate threats while identifying non-threats caused by these cases of overlapping local area networks.

The FCC recognizes and values the significant experience that DHS and other federal partners bring to this crucial cybersecurity discussion, and the FCC and DHS regularly share expertise in support of our independent yet complementary missions. The FCC enjoys a longstanding and mutually-beneficial working relationship with DHS and other interagency partners.

Thank you for your interest in this matter. The security of our nation's communications network is vital to both private and public sectors. We recognize that there is additional work to do to define defensible best practices for shared unlicensed bands, and we look forward to working with our federal partners to develop these best practices.

Sincerely,



Tom Wheeler