

Congress of the United States
House of Representatives
Washington, D.C. 20515

June 26, 2017

The Honorable Ajit V. Pai
Chairman
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

The Honorable Mignon L. Clyburn
Commissioner
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

The Honorable Michael O’Rielly
Commissioner
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

Dear Chairman Pai, Commissioner Clyburn, and Commissioner O’Rielly:

We write to express concerns about the Federal Communications Commission’s (FCC) cybersecurity preparedness, and the multiple reported problems with the FCC’s website in taking public comments in the net neutrality proceeding. Recent events have raised questions about the security of the FCC’s network, and we have serious concerns that the FCC’s website failures deprive the public of opportunities to comment on net neutrality – an issue that affects everyone who uses the internet.

Problems with the FCC’s net neutrality docket made headlines last month after comedian John Oliver implored his viewers to file comments about net neutrality with the FCC. Multiple media outlets reported that the FCC’s Electronic Comment Filing System “went down”¹ after the segment, noting that “the FCC’s servers appeared to be overwhelmed by the flood of traffic.”²

The following day, on May 8, 2017, the FCC’s Chief Information Officer announced that the FCC “was subject to multiple distributed denial-of-service attacks,” a situation that made it

¹ Ali Breland, *FCC site crashes after John Oliver segment*, The Hill (May 8, 2017). See also, Sam Gustin, *John Oliver Just Crashed the FCC’s Website Over Net Neutrality—Again*, Motherboard (May 8, 2017).

² Jeff John Roberts, *John Oliver Gets Fired Up Over Net Neutrality—and FCC’s Site Goes Down*, Fortune (May 8, 2017).

The Honorable Ajit V. Pai
The Honorable Mignon L. Clyburn
The Honorable Michael O'Rielly
June 26, 2017
Page 2

“difficult for legitimate commenters to access and file with the FCC.”³ In response to an inquiry from Senators Wyden and Schatz, the FCC recently released more information about the alleged cyberattacks.⁴ Yet the FCC’s response raises additional questions, and there are other areas of concern about the net neutrality docket for which we seek answers.

For example, recent reports have also indicated that as many as 150,000 comments had disappeared from the FCC’s net neutrality docket,⁵ and that automated comments were submitted to the FCC using names and addresses of real people without their knowledge or consent.⁶ Even with all of these problems and irregularities, the FCC has given only until the middle of August for the public to provide initial comments on the FCC’s net neutrality proposal, despite receiving calls to extend the deadline.⁷ Further, Republican Congressional leaders have not held hearings to examine these issues, despite receiving calls to do so.⁸

We ask you to examine these serious problems and irregularities that raise doubts about the fairness, and perhaps even the legitimacy, of the FCC’s process in its net neutrality proceeding. Giving the public an opportunity to comment in an open proceeding such as this one is crucial – so that the FCC can consider the full impact of its proposals, and treat everyone who would be affected fairly. It is also required by law. The FCC must comply with Administrative

³ Federal Communications Commission, *FCC CIO Statement on Distributed Denial-of-Service Attacks on FCC Electronic Comment Filing System* (May 8, 2017) (press release).

⁴ Letter from Ajit V. Pai, Chairman, Federal Communications Commission, to Senators Wyden and Schatz (June 15, 2017) (<https://www.politicopro.com/f/?id=0000015c-d59b-de74-a17f-ddbba4380001>) (FCC Response).

⁵ John Eggerton, *FCC’s Network Neutrality Docket Appears to Shrink*, Broadcasting & Cable (June 8, 2017).

⁶ Dominic Rushe, *‘Pretty ridiculous’: thousands of names stolen to attack net neutrality rules*, The Guardian (May 26, 2017).

⁷ Letter from Rep. Frank Pallone, Jr., Ranking Member, House Committee on Energy and Commerce, and Rep. Mike Doyle, Ranking Member, Subcommittee on Communications and Technology, House Committee on Energy and Commerce, to Ajit V. Pai, Chairman, Federal Communications Commission (May 11, 2017).

⁸ Letter from Rep. Frank Pallone, Jr., Ranking Member, House Committee on Energy and Commerce, Rep. Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, Rep. Mike Doyle, Ranking Member, Subcommittee on Communications and Technology, House Committee on Energy and Commerce, and Yvette Clarke, Member of Congress, to Rep. Greg Walden, Chairman, House Committee on Energy and Commerce, Rep. Tim Murphy, Chairman, Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, and Rep. Marsha Blackburn, Chairman, Subcommittee on Communications and Technology, House Committee on Energy and Commerce (May 17, 2017).

Procedure Act requirements to give the public notice and an opportunity to comment, as well as to respond to those comments.⁹ This is important, especially where the FCC is considering changing rules that affect everyone who uses the internet.

It is also critical that the FCC take all appropriate measures to secure its networks from cyberattacks. At a minimum, the FCC must meet cybersecurity requirements under the Federal Information Security Modernization Act (FISMA). The Chairman of the FCC is ultimately responsible under FISMA to provide information security protections for the agency.¹⁰ This is especially important given that the FCC’s Chief Information Officer stated that the FCC experienced a cyberattack that made it difficult for members of the public to file comments with the agency in an open proceeding.¹¹ We therefore request responses to the following questions by July 17, 2017:

1. According to the FCC’s response to Senators Wyden and Schatz, the May 2017 incident was a “non-traditional DDoS attack” where bot traffic “increased exponentially” between 11pm EST on May 7, 2017 until 1pm EST on May 8, 2017, representing a “3,000% increase in normal volume.”¹² What “additional solutions” is the FCC pursuing to “further protect the system,” as was mentioned in the FCC’s response?¹³
2. According to the FCC, the alleged cyberattacks blocked “new human visitors.... from visiting the comment filing system.”¹⁴ Yet, the FCC, consulting with the FBI, determined that “the attack did not rise to the level of a major incident that would trigger further FBI involvement.”¹⁵ What analysis did the FCC and the FBI conduct to determine that this was not a “major incident?”

⁹ 5 U.S.C. § 553. *See, e.g., Am. Radio Relay League, Inc. v. FCC*, 524 F.3d 227 (D.C. Cir) (2007) (remanding final rule to the FCC after finding the FCC had failed to comply with obligation under the Administrative Procedure Act to give interested parties notice and a reasonable opportunity to comment in the rulemaking process); *Home Box Office, Inc. v. FCC*, 567 F.2d 9 (D.C. Cir.) (1977) (vacating rule for failure of the FCC to comply with the Administrative Procedure Act’s notice and comment requirements that are intended to “provide fair treatment for persons affected by a rule.”).

¹⁰ 44 U.S.C. § 3554(a).

¹¹ FCC Press Release, *supra* n. 3.

¹² FCC Response, *supra* n. 4.

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

The Honorable Ajit V. Pai
The Honorable Mignon L. Clyburn
The Honorable Michael O'Rielly
June 26, 2017
Page 4

3. What specific "hardware resources" will the FCC commit to accommodate people attempting to file comments during high-profile proceedings? Does the FCC have sufficient resources for that purpose?
4. Is the FCC making alternative ways available for members of the public to file comments in the net neutrality proceeding?
5. Did the FCC contact the National Cybersecurity and Communications Integration Center's Hunt and Incident Response Team (HIRT) at the U.S. Department of Homeland Security to investigate the May 8, 2017 incident, and if so, on which date(s) was such contact made? If the FCC did not contact HIRT to investigate the May 8, 2017 incident, please explain why it did not do so.
6. What were the findings from any forensic investigative analyses or reports concerning the May 8, 2017 incident, including how and why a denial-of-service attacks were declared, and from what attack vectors they came?
7. Did the FCC notify Congress of the May 8, 2017 incidents as provided by FISMA?¹⁶ If so, how did the FCC notify Congress? If not, why not?
8. Did the FCC notify its Office of Inspector General (OIG) of the May 8, 2017 incidents, and if so, when did it notify the OIG?

Your assistance in this matter is greatly appreciated, and we look forward to receiving a response. If you have any questions, please contact the minority committee staff of the House Energy and Commerce Committee at (202) 225-3641 and the minority committee staff of the House Oversight and Government Reform Committee at (202) 225-5051.

Sincerely,



Frank Pallone, Jr.
Ranking Member
Committee on Energy
and Commerce



Elijah E. Cummings
Ranking Member
Committee on Oversight
and Government Reform

¹⁶ 44 U.S.C. § 3554(b)(7)(C)(iii)(III).

The Honorable Ajit V. Pai
The Honorable Mignon L. Clyburn
The Honorable Michael O'Rielly
June 26, 2017
Page 5



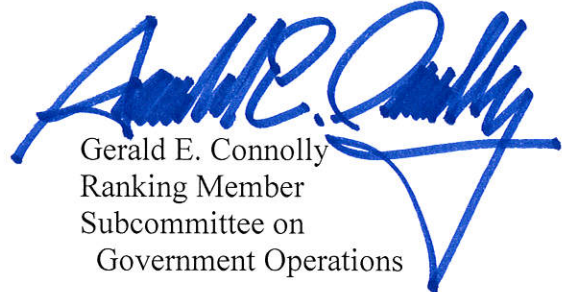
Diana DeGette
Ranking Member
Subcommittee on Oversight and
Investigations



Robin L. Kelly
Ranking Member
Subcommittee on
Information Technology



Mike Doyle
Ranking Member
Subcommittee on Communications
and Technology



Gerald E. Connolly
Ranking Member
Subcommittee on
Government Operations

Cc: The Honorable Trey Gowdy, Chairman
House Committee on Oversight and Government Reform

The Honorable Greg Walden, Chairman
House Committee on Energy and Commerce