

# Appendix A

May 07 20:22:20 Posting comment submission to FCC docket...  
May 07 20:27:19 Posting comment submission to FCC docket...  
May 07 20:27:29 Posting comment submission to FCC docket...  
May 07 20:28:26 Posting comment submission to FCC docket...  
May 07 20:29:02 Posting comment submission to FCC docket...  
May 07 20:29:03 status\_code: 503  
May 07 20:29:03 reason: Service Unavailable  
May 07 20:32:18 Posting comment submission to FCC docket...  
May 07 20:32:18 status\_code: 503  
May 07 20:32:18 reason: Service Unavailable  
May 07 20:33:29 Posting comment submission to FCC docket...  
May 07 20:33:36 Posting comment submission to FCC docket...  
May 07 20:34:16 Posting comment submission to FCC docket...  
May 07 20:34:53 Posting comment submission to FCC docket...  
May 07 20:34:53 status\_code: 503  
May 07 20:34:53 reason: Service Unavailable  
May 07 20:35:00 Posting comment submission to FCC docket...  
May 07 20:35:23 Posting comment submission to FCC docket...  
May 07 20:35:23 status\_code: 503  
May 07 20:35:23 reason: Service Unavailable  
May 07 20:35:56 Posting comment submission to FCC docket...  
May 07 20:35:57 status\_code: 503  
May 07 20:35:57 reason: Service Unavailable  
May 07 20:38:03 Posting comment submission to FCC docket...  
May 07 20:38:03 status\_code: 503  
May 07 20:38:03 reason: Service Unavailable  
May 07 20:38:07 Posting comment submission to FCC docket...  
May 07 20:38:55 Posting comment submission to FCC docket...  
May 07 20:39:23 Posting comment submission to FCC docket...  
May 07 20:39:23 status\_code: 503  
May 07 20:39:23 reason: Service Unavailable  
May 07 20:39:52 Posting comment submission to FCC docket...  
May 07 20:39:52 status\_code: 503  
May 07 20:39:52 reason: Service Unavailable  
May 07 20:40:11 Posting comment submission to FCC docket...  
May 07 20:40:12 status\_code: 503  
May 07 20:40:12 reason: Service Unavailable  
May 07 20:40:49 Posting comment submission to FCC docket...  
May 07 20:40:49 status\_code: 503  
May 07 20:40:49 reason: Service Unavailable  
May 07 20:41:17 Posting comment submission to FCC docket...  
May 07 20:41:17 status\_code: 503  
May 07 20:41:17 reason: Service Unavailable  
May 07 20:41:20 Posting comment submission to FCC docket...  
May 07 20:41:20 status\_code: 503  
May 07 20:41:20 reason: Service Unavailable

May 08 17:28:52 Posting comment submission to FCC docket...  
May 08 17:29:01 Posting comment submission to FCC docket...  
May 08 17:29:03 Posting comment submission to FCC docket...  
May 08 17:29:09 Posting comment submission to FCC docket...  
May 08 17:29:55 Posting comment submission to FCC docket...  
May 08 17:30:08 Posting comment submission to FCC docket...  
May 08 17:30:08 status\_code: 503  
May 08 17:30:08 reason: Service Unavailable  
May 08 17:30:08 Posting comment submission to FCC docket...  
May 08 17:30:09 status\_code: 503  
May 08 17:30:09 reason: Service Unavailable  
May 08 17:30:09 Posting comment submission to FCC docket...  
May 08 17:30:10 status\_code: 503  
May 08 17:30:10 reason: Service Unavailable  
May 08 17:30:10 Posting comment submission to FCC docket...  
May 08 17:30:10 status\_code: 503  
May 08 17:30:10 reason: Service Unavailable  
May 08 17:30:11 Posting comment submission to FCC docket...  
May 08 17:30:11 status\_code: 503  
May 08 17:30:11 reason: Service Unavailable  
May 08 17:30:11 Posting comment submission to FCC docket...  
May 08 17:30:12 Posting comment submission to FCC docket...  
May 08 17:30:12 status\_code: 503  
May 08 17:30:12 reason: Service Unavailable  
May 08 17:30:12 status\_code: 503  
May 08 17:30:12 reason: Service Unavailable  
May 08 17:30:13 Posting comment submission to FCC docket...  
May 08 17:30:13 Posting comment submission to FCC docket...  
May 08 17:30:13 status\_code: 503  
May 08 17:30:13 reason: Service Unavailable  
May 08 17:30:13 status\_code: 503  
May 08 17:30:13 reason: Service Unavailable  
May 08 17:30:13 Posting comment submission to FCC docket...  
May 08 17:30:14 status\_code: 503  
May 08 17:30:14 reason: Service Unavailable  
May 08 17:30:32 Posting comment submission to FCC docket...  
May 08 17:30:33 status\_code: 503  
May 08 17:30:33 reason: Service Unavailable

May 08 06:28:14 reason: Service Unavailable  
May 08 06:28:20 Posting comment submission to FCC docket...  
May 08 06:28:20 status\_code: 503  
May 08 06:28:20 reason: Service Unavailable  
May 08 06:29:29 Posting comment submission to FCC docket...  
May 08 06:29:43 Posting comment submission to FCC docket...  
May 08 06:29:44 status\_code: 503  
May 08 06:29:44 reason: Service Unavailable  
May 08 06:31:30 Posting comment submission to FCC docket...  
May 08 06:31:30 status\_code: 503  
May 08 06:31:30 reason: Service Unavailable  
May 08 06:32:20 Posting comment submission to FCC docket...  
May 08 06:32:20 status\_code: 503  
May 08 06:32:20 reason: Service Unavailable  
May 08 06:33:47 Posting comment submission to FCC docket...  
May 08 06:33:47 status\_code: 503  
May 08 06:33:47 reason: Service Unavailable  
May 08 06:37:21 Posting comment submission to FCC docket...  
May 08 06:37:22 Posting comment submission to FCC docket...  
May 08 06:37:32 Posting comment submission to FCC docket...  
May 08 06:38:44 Posting comment submission to FCC docket...  
May 08 06:38:56 Posting comment submission to FCC docket...  
May 08 06:39:20 Posting comment submission to FCC docket...  
May 08 06:39:24 Posting comment submission to FCC docket...  
May 08 06:39:24 status\_code: 503  
May 08 06:39:24 reason: Service Unavailable  
May 08 06:40:50 Posting comment submission to FCC docket...  
May 08 06:43:45 Posting comment submission to FCC docket...  
May 08 06:45:19 Posting comment submission to FCC docket...  
May 08 06:45:19 status\_code: 503  
May 08 06:45:19 reason: Service Unavailable  
May 08 06:45:22 Posting comment submission to FCC docket...  
May 08 06:45:29 Posting comment submission to FCC docket...  
May 08 06:45:34 Posting comment submission to FCC docket...  
May 08 06:47:54 Posting comment submission to FCC docket...  
May 08 06:47:55 Posting comment submission to FCC docket...  
May 08 06:50:28 Posting comment submission to FCC docket...  
May 08 06:52:18 Posting comment submission to FCC docket...  
May 08 06:52:47 Posting comment submission to FCC docket...  
May 08 06:53:01 Posting comment submission to FCC docket...  
May 08 06:53:03 Posting comment submission to FCC docket...  
May 08 06:53:19 Posting comment submission to FCC docket...  
May 08 06:53:26 Posting comment submission to FCC docket...  
May 08 06:53:32 Posting comment submission to FCC docket...  
May 08 06:55:46 Posting comment submission to FCC docket...  
May 08 06:57:49 Posting comment submission to FCC docket...

# Appendix B

RON WYDEN  
OREGON

RANKING MEMBER OF COMMITTEE ON  
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING  
WASHINGTON, DC 20510  
(202) 224-5244

**United States Senate**  
WASHINGTON, DC 20510-3703

**COMMITTEES:**

COMMITTEE ON FINANCE  
COMMITTEE ON BUDGET  
COMMITTEE ON ENERGY & NATURAL RESOURCES  
SELECT COMMITTEE ON INTELLIGENCE  
JOINT COMMITTEE ON TAXATION

May 9, 2017

387

The Honorable Ajit Pai  
Chairman  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, DC 20554

Dear Chairman Pai:

According to your May 8 press release, you claim the Federal Communications Commission (FCC) has recently been the victim of “multiple distributed denial-of-service attacks (DDoS)”. DDoS attacks against federal agencies are serious—and doubly so if the attack may have prevented Americans from being able to weigh in on your proposal to roll back net neutrality protections.

As you know, it is critical to the rulemaking and regulatory process that the public be able to take part without unnecessary technical or administrative burdens. A denial-of-service attack against the FCC’s website can prevent the public from being able to contribute to this process and have their voices heard. Any potentially hostile cyber activities that prevent Americans from being able to participate in a fair and transparent process must be treated as a serious issue. As such, we ask you to keep Congress fully briefed as to your investigation. Please, by June 8, 2017 answer the following questions.

In the meantime, please make available alternative ways for the public to comment; for example, a dedicated email account on the net neutrality proceeding as was done in 2014.

1. Please provide details as to the nature of the DDoS attacks, including when the attacks began, when they ended, the amount of malicious traffic your network received, and an estimate of the number of devices that were sending malicious traffic to the FCC. To the extent that the FCC already has evidence suggesting which actor(s) may have been responsible for the attacks, please provide that in your response.
2. Has the FCC sought assistance from other federal agencies in investigating and responding to these attacks? Which agencies have you sought assistance from? Have you received all of the help you have requested?
3. Several federal agencies utilize commercial services to protect their websites from DDoS attacks. Does the FCC use a commercial DDoS protection service? If not, why not? To

911 NE 11TH AVENUE  
SUITE 630  
PORTLAND, OR 97232  
(503) 326-7525

405 EAST 8TH AVE  
SUITE 2020  
EUGENE, OR 97401  
(541) 431-0229

SAC ANNEX BUILDING  
105 HR ST  
SUITE 201  
LA GRANDE, OR 97350  
(541) 962-7691

U.S. COURTHOUSE  
310 WEST 6TH ST  
ROOM 118  
MEDFORD, OR 97501  
(541) 858-5122

THE JAMISON BUILDING  
131 NW HAWTHORNE AVE  
SUITE 107  
BEND, OR 97701  
(541) 330-9142

707 13TH ST. SE  
SUITE 285  
SALEM, OR 97301  
(503) 589-4555

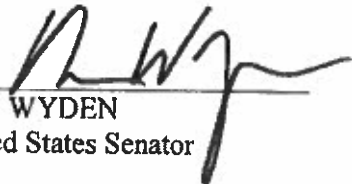
[HTTP://WYDEN.SENATE.GOV](http://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

the extent that the FCC utilizes commercial DDoS protection products, did these work as expected? If not, why not?

4. How many concurrent visitors is the FCC's website designed to be able to handle? Has the FCC performed stress testing of its own website to ensure that it can cope as intended? Has the FCC identified which elements of its website are performance bottlenecks that limit the number of maximum concurrent visitors? Has the FCC sought to mitigate these bottlenecks? If not, why not?
5. Did the DDoS attacks prevent the public from being able to submit comments through the FCC's website? If so, do you have an estimate of how many individuals were unable to access the FCC website or submit comments during the attacks? Were any comments lost or otherwise affected?
6. Will commenters who successfully submitted a comment—but did not receive a response, as your press release indicates—receive a response once your staff have addressed the DDoS and related technical issues?
7. Does the FCC have all of the resources and expertise it needs in order to combat attacks like those that occurred on May 8?

Sincerely,

  
RON WYDEN  
United States Senator

  
BRIAN SCHATZ  
United States Senator



OFFICE OF  
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

June 15, 2017

The Honorable Ron Wyden  
United States Senate  
221 Dirksen Senate Office Building  
Washington, D.C. 20510

Dear Senator Wyden:

This letter responds to your May 9, 2017, correspondence and questions concerning the Federal Communications Commission's (FCC) response to the May 7-8, 2017, cyber-based attack against its Electronic Comment Filing System (ECFS). I agree that this disruption to ECFS by outside parties was a very serious matter. As a result, my office immediately directed our Chief Information Officer (CIO) to take appropriate measures to secure the integrity of ECFS and to keep us apprised of the situation.

The Commission's CIO has informed me that the FCC's response to the events sufficiently addressed the disruption, and that ECFS is continuing to collect all filed comments. Indeed, as of this date, we have received more than 4.98 million comments in this proceeding—the most the FCC has ever received for any proceeding through ECFS.

Please be assured that I have directed the Commission's Information Technology (IT) staff to continue to closely monitor ECFS and expeditiously address and report any potential issues to my office. IT staff provide regular reports of the current state of our network operations (including any incipient threats), as well as incoming comment numbers and work to provide an uninterrupted, transparent, and quality experience for all stakeholders.

The CIO has provided me with the attached answers to your questions in the above-referenced correspondence. Please let me know if I can be of any further assistance.

Sincerely,

A handwritten signature in black ink, appearing to read "Ajit V. Pai".

Ajit V. Pai

Enclosure



## ATTACHMENT

**1. Please provide details as to the nature of the DDoS attacks, including when the attacks began, when they ended, the amount of malicious traffic your network received, and an estimate of the number of devices that were sending malicious traffic to the FCC. To the extent that the FCC already has evidence suggesting which actor(s) may have been responsible for the attacks, please provide that in your response.**

We have determined that this disruption is best classified as a non-traditional DDoS attack. Specifically, the disrupters targeted the comment filing system application programming interface (API), which is distinct from the website, and is normally used by automated programs or bots for bulk filings.

Our decision to classify the nature of the attack as a non-traditional DDoS is based on specific data as well as a pattern of disruptions that show abnormal behavior outside the scope of a lobbying surge. As discussed below, we detected an extremely high level of atypical cloud-based traffic accessing the API interface, but very few of these connections actually left comments. These automated programs or bots operated in a way that precluded human user access to the system.

The peak activity triggering the comment system's unavailability to most human filers appears to have started at approximately 11:00 p.m. Eastern Standard Time (EST) on Sunday, May 7, 2017. Bot traffic to the system's API increased exponentially from 11:00 p.m. EST to May 8, 2017, at 1:00 a.m. EST. In fact, the number of hits on the comment filing system's API increased from three to five requests per second to over 160 requests per second, representing a 3,000% increase in normal volume. Moreover, we would note that when John Oliver provided a link to encourage viewers to file comments on the evening of Sunday, May 7, 2017, that link directed traffic to the regular comment filing system and not to the API.

From our analysis of the logs, we believe these automated bot programs appeared to be cloud-based and not associated with IP addresses usually linked to individual human filers. We found that the bots initiated API requests with the system and then via their high-speed, resource-intensive requests, effectively blocked or denied additional web traffic—human or otherwise—to the comment filing system. Since both humans and bots were attempting to access the same system and because bots could make more intensive resource requests much faster than humans, the “bot surge” triggered the comment filing system to queue and ultimately decline new connections. The result was that new human users were blocked from visiting the comment filing system.

By 1:00 a.m. EST on Monday, May 8, 2017, the system effectively reduced the number of new requests it would accept in response to the bot swarm. We believe that these bot swarms continued, peaking at 30,000 requests per minute, or three times the total daily traffic for any day in the previous sixty days. This volume also represented the maximum volume that the commercial, cloud-based API servers could handle.

Unfortunately, it would have been exceedingly difficult by 1:00 a.m. EST for new filers to make a new connection until after we initiated our mitigation efforts at 6:00 a.m. EST and sufficiently increased capacity by the start of business hours at 8:45 a.m. EST. By 8:45 a.m. EST, the Commission had increased the filing system's API capacity to over 400 hits per second.

It is important to note that the Commission did not have the technical option of blocking or removing the bots hitting the API. By increasing API capacity, the Commission permitted the system to respond to new human users who had been denied access since the bots were able to use their speed to make more intensive resource requests than humans.

In addition to the basic findings above, our IT staff found other markers of potential malicious intent. For instance, the bots included API calls that were structured—that is, API calls designed not to submit comments, but merely to create an artificial demand for additional resources on the cloud-based system. This appears to have been designed to impede the performance of the comment filing system's components. Later analysis showed the perpetrators requested multiple keys associated with individual IP addresses. This action bypassed the normal protection that prevents such a surge from denying access to human users.

We are unable to determine the total amount of malicious traffic experienced, but we continue to research the number of devices involved in and the origin of the bot swarms. Since the bot traffic emanated from cloud providers, determining the actual source is more difficult than finding that of individual submittals tied to an IP address used by humans.

Importantly, the system remained secure and nothing was hacked. In addition, the FCC successfully received more than two million comments in 10 days, versus more than two million comments over 110 days in the related 2014-15 proceeding. This number includes a one-day record of more than 400,000 comments on Thursday, May 11, 2017. We continue to research additional solutions to strengthen ECFS' controls to further protect the system.

**2. Has the FCC sought assistance from other federal agencies in investigating and responding to these attacks? Which agencies have you sought assistance from? Have you received all of the help you have requested?**

Following this attack, the FCC CIO directed the Chief Information Security Officer (CISO) to consult with the FBI. In speaking with the FBI, the conclusion was reached that, given the facts currently known, the attack did not appear to rise to the level of a major incident that would trigger further FBI involvement. The FCC and FBI agreed to have further discussions if additional events or the discovery of additional evidence warrant consultation.

**3. Several federal agencies utilize commercial services to protect their websites from DDoS attacks. Does the FCC use a commercial DDoS protection service? If not, why not? To the extent that the FCC utilizes commercial DDoS protection products, did these work as expected? If not, why not?**

Yes, the FCC has several commercially provided services and tools to protect its systems from DDoS attacks as well as all forms of cyber-attacks. The non-traditional DDoS that we

experienced is quite different than typical attacks in that it used legitimate commercial providers to introduce bots and poorly structured queries to overload the system.

Because the FCC is required to accept comments in virtually any form and from any source, our commercial providers are severely limited in the actions they may take to shut down what are perceived as inappropriate or malicious bots accessing system resources. However, the FCC did implement a rate limit on its API to prevent any one bot from draining excessive system resources. But this rate is tied to a key, and if bots requested multiple keys, they could bypass the limit. We believe there were instances where a single IP address requested multiple keys, thus bypassing the rate limit.

The FCC IT team is considering more advanced solutions to preclude this situation in the future. To be sure, the products and providers that we used performed as expected. But this type of problem is ongoing in nature and requires focused resources to keep up with malicious players seeking to disrupt our work. The FCC will continue to use its available resources to respond to these attempts to disrupt our systems.

#### **4. How many concurrent visitors is the FCC's website designed to be able to handle?**

The exact number is unknown, as cloud-based systems are not built with a set number of "visitors"—either human or automated programs (bots). Also, what the visitors are doing while they visit a website, such as the size of visitor inputs to and output requests from the system, influences the potential drain on system resources.

The FCC moved ECFS to a cloud infrastructure to allow for scaling in the event of a large number of inputs and requests. This scaling still requires human involvement in load-balancing and related activities. The FCC successfully received a record of more than 400,000 comments in one day on Thursday, May 11, 2017—showing the system can scale to accommodate a large number of visitors when other external factors are not present. An average day sees closer to 10,000 comments a day, which is why ECFS is cloud-based—to address sudden surges.

##### **A. Has the FCC performed stress testing of its own website to ensure that it can cope as intended?**

The FCC stress tests to the extent possible, but cannot anticipate all scenarios. The system has operated as intended when malicious acts are not being committed to disrupt its operations.

##### **B. Has the FCC identified which elements of its website are performance bottlenecks that limit the number of maximum concurrent visitors?**

Access to the website was not the issue, so the number count on the front of the website was not relevant. In this case, the problem arose through the misuse of an API that is available on the FCC's website.

##### **C. Has the FCC sought to mitigate these bottlenecks? If not, why not?**

Yes. The FCC has committed resources to mitigate the issue that occurred. The FCC will commit more hardware resources to handle requests that threaten the ability of the system to be responsive. The FCC also will continue to investigate newer and better technologies to identify and prevent resources from being occupied at the expense of legitimate filers.

**5. Did the DDoS attacks prevent the public from being able to submit comments through the FCC website? If so, do you have an estimate of how many individuals were unable to access the FCC website or submit comments during the attacks? Were any comments lost or otherwise affected?**

During the bot swarms, which peaked in the early hours of May 8, 2017, the FCC addressed the problem to bring the system back to an acceptable level of performance within hours of the disruption. While we cannot count the number of “individuals” who might have been delayed in their attempt to file comments during that time frame, we believe that the impact was mitigated by addressing the bot swarms promptly on May 8, 2017. Potential commenters would have been able to file later in the day or in the days that followed. Importantly, the comment cycle is still open, which means comments can still be filed. At this stage, we have received 4.98 million comments, so the comment filing system is clearly facilitating widespread participation in this proceeding.

**6. Will commenters who successfully submitted a comment—but did not receive a response, as your press release indicates—receive a response once your staff have addressed the DDoS and related technical issues?**

When a commenter files comments through the standard ECFS system, the commenter receives an immediate confirmation number on the screen. Commenters who did not record their number or are unsure if their comments have been received may initiate a name search to confirm that their comments have been filed. If the commenter’s name does not appear in the system, the commenter should refile and record the confirmation number.

**7. Does the FCC have all of the resources and expertise it needs in order to combat attacks like those that occurred on May 8?**

Although the FCC has demonstrated the resiliency of its systems, we must be consistently vigilant in safeguarding IT assets to ensure system availability for all constituents. The FCC is dependent upon its IT team to deal with any issues that may occur going forward and they are continuing to explore potential improvements to the system. If the Commission needs additional resources to address system and cybersecurity issues, we will work with OMB and the Appropriations Committees to ensure that we have the funds to undertake essential upgrades.



OFFICE OF  
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

June 15, 2017

The Honorable Brian Schatz  
United States Senate  
722 Hart Senate Office Building  
Washington, D.C. 20510

Dear Senator Schatz:

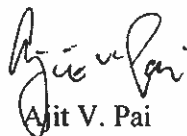
This letter responds to your May 9, 2017, correspondence and questions concerning the Federal Communications Commission's (FCC) response to the May 7-8, 2017, cyber-based attack against its Electronic Comment Filing System (ECFS). I agree that this disruption to ECFS by outside parties was a very serious matter. As a result, my office immediately directed our Chief Information Officer (CIO) to take appropriate measures to secure the integrity of ECFS and to keep us apprised of the situation.

The Commission's CIO has informed me that the FCC's response to the events sufficiently addressed the disruption, and that ECFS is continuing to collect all filed comments. Indeed, as of this date, we have received more than 4.98 million comments in this proceeding—the most the FCC has ever received for any proceeding through ECFS.

Please be assured that I have directed the Commission's Information Technology (IT) staff to continue to closely monitor ECFS and expeditiously address and report any potential issues to my office. IT staff provide regular reports of the current state of our network operations (including any incipient threats), as well as incoming comment numbers and work to provide an uninterrupted, transparent, and quality experience for all stakeholders.

The CIO has provided me with the attached answers to your questions in the above-referenced correspondence. Please let me know if I can be of any further assistance.

Sincerely,

  
Ajit V. Pai

Enclosure

## ATTACHMENT

**1. Please provide details as to the nature of the DDoS attacks, including when the attacks began, when they ended, the amount of malicious traffic your network received, and an estimate of the number of devices that were sending malicious traffic to the FCC. To the extent that the FCC already has evidence suggesting which actor(s) may have been responsible for the attacks, please provide that in your response.**

We have determined that this disruption is best classified as a non-traditional DDoS attack. Specifically, the disrupters targeted the comment filing system application programming interface (API), which is distinct from the website, and is normally used by automated programs or bots for bulk filings.

Our decision to classify the nature of the attack as a non-traditional DDoS is based on specific data as well as a pattern of disruptions that show abnormal behavior outside the scope of a lobbying surge. As discussed below, we detected an extremely high level of atypical cloud-based traffic accessing the API interface, but very few of these connections actually left comments. These automated programs or bots operated in a way that precluded human user access to the system.

The peak activity triggering the comment system's unavailability to most human filers appears to have started at approximately 11:00 p.m. Eastern Standard Time (EST) on Sunday, May 7, 2017. Bot traffic to the system's API increased exponentially from 11:00 p.m. EST to May 8, 2017, at 1:00 a.m. EST. In fact, the number of hits on the comment filing system's API increased from three to five requests per second to over 160 requests per second, representing a 3,000% increase in normal volume. Moreover, we would note that when John Oliver provided a link to encourage viewers to file comments on the evening of Sunday, May 7, 2017, that link directed traffic to the regular comment filing system and not to the API.

From our analysis of the logs, we believe these automated bot programs appeared to be cloud-based and not associated with IP addresses usually linked to individual human filers. We found that the bots initiated API requests with the system and then via their high-speed, resource-intensive requests, effectively blocked or denied additional web traffic—human or otherwise—to the comment filing system. Since both humans and bots were attempting to access the same system and because bots could make more intensive resource requests much faster than humans, the “bot surge” triggered the comment filing system to queue and ultimately decline new connections. The result was that new human users were blocked from visiting the comment filing system.

By 1:00 a.m. EST on Monday, May 8, 2017, the system effectively reduced the number of new requests it would accept in response to the bot swarm. We believe that these bot swarms continued, peaking at 30,000 requests per minute, or three times the total daily traffic for any day in the previous sixty days. This volume also represented the maximum volume that the commercial, cloud-based API servers could handle.

Unfortunately, it would have been exceedingly difficult by 1:00 a.m. EST for new filers to make a new connection until after we initiated our mitigation efforts at 6:00 a.m. EST and sufficiently increased capacity by the start of business hours at 8:45 a.m. EST. By 8:45 a.m. EST, the Commission had increased the filing system's API capacity to over 400 hits per second.

It is important to note that the Commission did not have the technical option of blocking or removing the bots hitting the API. By increasing API capacity, the Commission permitted the system to respond to new human users who had been denied access since the bots were able to use their speed to make more intensive resource requests than humans.

In addition to the basic findings above, our IT staff found other markers of potential malicious intent. For instance, the bots included API calls that were structured—that is, API calls designed not to submit comments, but merely to create an artificial demand for additional resources on the cloud-based system. This appears to have been designed to impede the performance of the comment filing system's components. Later analysis showed the perpetrators requested multiple keys associated with individual IP addresses. This action bypassed the normal protection that prevents such a surge from denying access to human users.

We are unable to determine the total amount of malicious traffic experienced, but we continue to research the number of devices involved in and the origin of the bot swarms. Since the bot traffic emanated from cloud providers, determining the actual source is more difficult than finding that of individual submittals tied to an IP address used by humans.

Importantly, the system remained secure and nothing was hacked. In addition, the FCC successfully received more than two million comments in 10 days, versus more than two million comments over 110 days in the related 2014-15 proceeding. This number includes a one-day record of more than 400,000 comments on Thursday, May 11, 2017. We continue to research additional solutions to strengthen ECFS' controls to further protect the system.

**2. Has the FCC sought assistance from other federal agencies in investigating and responding to these attacks? Which agencies have you sought assistance from? Have you received all of the help you have requested?**

Following this attack, the FCC CIO directed the Chief Information Security Officer (CISO) to consult with the FBI. In speaking with the FBI, the conclusion was reached that, given the facts currently known, the attack did not appear to rise to the level of a major incident that would trigger further FBI involvement. The FCC and FBI agreed to have further discussions if additional events or the discovery of additional evidence warrant consultation.

**3. Several federal agencies utilize commercial services to protect their websites from DDoS attacks. Does the FCC use a commercial DDoS protection service? If not, why not? To the extent that the FCC utilizes commercial DDoS protection products, did these work as expected? If not, why not?**

Yes, the FCC has several commercially provided services and tools to protect its systems from DDoS attacks as well as all forms of cyber-attacks. The non-traditional DDoS that we

experienced is quite different than typical attacks in that it used legitimate commercial providers to introduce bots and poorly structured queries to overload the system.

Because the FCC is required to accept comments in virtually any form and from any source, our commercial providers are severely limited in the actions they may take to shut down what are perceived as inappropriate or malicious bots accessing system resources. However, the FCC did implement a rate limit on its API to prevent any one bot from draining excessive system resources. But this rate is tied to a key, and if bots requested multiple keys, they could bypass the limit. We believe there were instances where a single IP address requested multiple keys, thus bypassing the rate limit.

The FCC IT team is considering more advanced solutions to preclude this situation in the future. To be sure, the products and providers that we used performed as expected. But this type of problem is ongoing in nature and requires focused resources to keep up with malicious players seeking to disrupt our work. The FCC will continue to use its available resources to respond to these attempts to disrupt our systems.

#### **4. How many concurrent visitors is the FCC's website designed to be able to handle?**

The exact number is unknown, as cloud-based systems are not built with a set number of "visitors"—either human or automated programs (bots). Also, what the visitors are doing while they visit a website, such as the size of visitor inputs to and output requests from the system, influences the potential drain on system resources.

The FCC moved ECFS to a cloud infrastructure to allow for scaling in the event of a large number of inputs and requests. This scaling still requires human involvement in load-balancing and related activities. The FCC successfully received a record of more than 400,000 comments in one day on Thursday, May 11, 2017—showing the system can scale to accommodate a large number of visitors when other external factors are not present. An average day sees closer to 10,000 comments a day, which is why ECFS is cloud-based—to address sudden surges.

##### **A. Has the FCC performed stress testing of its own website to ensure that it can cope as intended?**

The FCC stress tests to the extent possible, but cannot anticipate all scenarios. The system has operated as intended when malicious acts are not being committed to disrupt its operations.

##### **B. Has the FCC identified which elements of its website are performance bottlenecks that limit the number of maximum concurrent visitors?**

Access to the website was not the issue, so the number count on the front of the website was not relevant. In this case, the problem arose through the misuse of an API that is available on the FCC's website.

##### **C. Has the FCC sought to mitigate these bottlenecks? If not, why not?**



Yes. The FCC has committed resources to mitigate the issue that occurred. The FCC will commit more hardware resources to handle requests that threaten the ability of the system to be responsive. The FCC also will continue to investigate newer and better technologies to identify and prevent resources from being occupied at the expense of legitimate filers.

**5. Did the DDoS attacks prevent the public from being able to submit comments through the FCC website? If so, do you have an estimate of how many individuals were unable to access the FCC website or submit comments during the attacks? Were any comments lost or otherwise affected?**

During the bot swarms, which peaked in the early hours of May 8, 2017, the FCC addressed the problem to bring the system back to an acceptable level of performance within hours of the disruption. While we cannot count the number of “individuals” who might have been delayed in their attempt to file comments during that time frame, we believe that the impact was mitigated by addressing the bot swarms promptly on May 8, 2017. Potential commenters would have been able to file later in the day or in the days that followed. Importantly, the comment cycle is still open, which means comments can still be filed. At this stage, we have received 4.98 million comments, so the comment filing system is clearly facilitating widespread participation in this proceeding.

**6. Will commenters who successfully submitted a comment—but did not receive a response, as your press release indicates—receive a response once your staff have addressed the DDoS and related technical issues?**

When a commenter files comments through the standard ECFS system, the commenter receives an immediate confirmation number on the screen. Commenters who did not record their number or are unsure if their comments have been received may initiate a name search to confirm that their comments have been filed. If the commenter’s name does not appear in the system, the commenter should refile and record the confirmation number.

**7. Does the FCC have all of the resources and expertise it needs in order to combat attacks like those that occurred on May 8?**

Although the FCC has demonstrated the resiliency of its systems, we must be consistently vigilant in safeguarding IT assets to ensure system availability for all constituents. The FCC is dependent upon its IT team to deal with any issues that may occur going forward and they are continuing to explore potential improvements to the system. If the Commission needs additional resources to address system and cybersecurity issues, we will work with OMB and the Appropriations Committees to ensure that we have the funds to undertake essential upgrades.

# Appendix C

# United States Senate

WASHINGTON, DC 20510

July 7, 2017

566

The Honorable Ajit V. Pai  
Chairman, Federal Communications Commission  
445 12<sup>th</sup> St. SW  
Washington, DC 20554

Dear Chairman Pai:

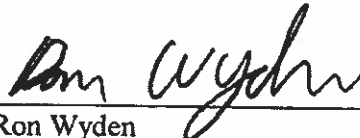
As you stated in your June 15 letter, the Federal Communications Commission (FCC) previously suffered a "non-traditional DDoS attack," which prevented the public from commenting on ongoing proceedings. We therefore write to ensure the FCC is prepared for the upcoming July 12 Day of Action to protect strong net neutrality rules.

On July 12, 2017, thousands of individuals will comment on Docket 17-108, a notice of proposed rulemaking that will roll back strong net neutrality protections, using the FCC's website or through a third-party. As we have stated previously, it is critical to the rulemaking and regulatory process that the public be able to take part without unnecessary technical or administrative burden. The FCC must be able to accept all comments filed to ensure that all voices are heard.

Many individuals submitting comments do so through a third-party that connects to your comment filing system application programming interface (API). As you stated in your letter, on May 7-8, the API for your Electronic Communication Filing System (ECFS) was disabled by what you refer to as a "non-traditional DDoS" attack, which left individuals unable to comment, even if they were not attempting to use your API. This was an unacceptable mistake that left Americans disenfranchised from your comment process.

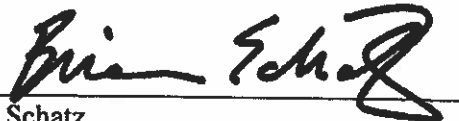
Due to the timing of the May 7-8 attack, which took place after a television host's call to action, we are concerned that a similar attack may be planned to disrupt the Day of Action. We encourage you to seek out and employ ECFS measures that allow for flexible scalability and alternative methods of filing. Additionally, if it is known internally that the ECFS will not be able to withstand an attack similar to the May 7-8 attack, we urge you to undertake temporary measures to ensure a functioning system on and around the anticipated surge of legitimate comments. In case the ECFS is disabled through some new type of attack, it is critical that Americans be able to file a comment using other means. We request that you make available an alternative mechanism for the public to file a comment including either through the FCC's own website and/or via a dedicated email address.

Thank you for your time and attention to this matter. Please respond to our staffs by July 11 indicating that necessary precautions are being taken. For any questions or clarifications, please contact Anderson Heiman of Senator Wyden's staff and Melika Carroll of Senator Schatz's staff.



Ron Wyden  
United States Senator

Sincerely,



Brian Schatz  
United States Senator



OFFICE OF  
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

July 11, 2017

The Honorable Ron Wyden  
United States Senate  
221 Dirksen Senate Office Building  
Washington, D.C. 20510

Dear Senator Wyden:

Thank you for your letter regarding the precautions that the Federal Communications Commission is taking to protect the FCC's comment filing process in advance of the expected activity on July 12 described in your letter. As I indicated in my June 15 letter to you, the cyber-based attack against the Commission's Electronic Comment Filing System (ECFS) on May 7-8 was a very serious matter. And in response to this incident, my office directed our Chief Information Officer to take measures to secure the integrity of the comment filing system and report back to us routinely on this work.

Over the course of the last two months, the Commission has taken a series of steps to mitigate the chances of a disruption similar to the one that took place on May 7-8 from occurring again. And during the comment period following the adoption of the Restoring Internet Freedom Notice of Proposed Rulemaking, our comment filing system has performed well to date. Indeed, the Commission has received over 600,000 comments in the last thirty days, and the docket now contains more than six million comments overall, demonstrating that the Commission's processes are facilitating widespread public participation in this proceeding.

In preparation for July 12, the Commission's IT professionals have taken additional measures to safeguard our comment filing system. Moreover, they will be on high alert over the next 48 hours and ready to respond as quickly as possible to any attacks. Given the nature of this situation, however, I believe that publicly disclosing the specific steps that we are taking could undermine their efficacy.

Of course, it is important to recognize that malicious actors seeking to cause disruptions have many tools at their disposal, as well. The Commission therefore cannot guarantee that any attacks launched against us will not have an impact.

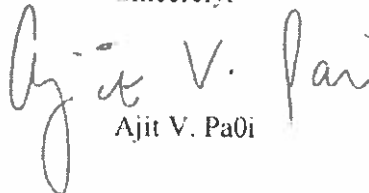
Filers wishing to submit comments to the FCC have four alternatives. They can file using the normal web interface. They can file through the API. They can submit comments using the electronic inbox and the Restoring Internet ECFS Bulk Upload Template. And they can submit a written comment. Should any of these methods be temporarily disrupted or unavailable, members of the public can use an alternative method or wait until the incident has ended. Given the length of time that the Commission has provided for public comment (90 days) as well as the multiple avenues available for submitting such comments, everyone seeking to

Page 2—The Honorable Ron Wyden

participate in this proceeding will have a chance to make his or her voice heard on this important subject.

I appreciate your interest in this matter.

Sincerely,

  
Ajit V. Paoli



OFFICE OF  
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

July 11, 2017

The Honorable Brian Schatz  
United States Senate  
722 Hart Senate Office Building  
Washington, D.C. 20510

Dear Senator Schatz:

Thank you for your letter regarding the precautions that the Federal Communications Commission is taking to protect the FCC's comment filing process in advance of the expected activity on July 12 described in your letter. As I indicated in my June 15 letter to you, the cyber-based attack against the Commission's Electronic Comment Filing System (ECFS) on May 7-8 was a very serious matter. And in response to this incident, my office directed our Chief Information Officer to take measures to secure the integrity of the comment filing system and report back to us routinely on this work.

Over the course of the last two months, the Commission has taken a series of steps to mitigate the chances of a disruption similar to the one that took place on May 7-8 from occurring again. And during the comment period following the adoption of the Restoring Internet Freedom Notice of Proposed Rulemaking, our comment filing system has performed well to date. Indeed, the Commission has received over 600,000 comments in the last thirty days, and the docket now contains more than six million comments overall, demonstrating that the Commission's processes are facilitating widespread public participation in this proceeding.

In preparation for July 12, the Commission's IT professionals have taken additional measures to safeguard our comment filing system. Moreover, they will be on high alert over the next 48 hours and ready to respond as quickly as possible to any attacks. Given the nature of this situation, however, I believe that publicly disclosing the specific steps that we are taking could undermine their efficacy.

Of course, it is important to recognize that malicious actors seeking to cause disruptions have many tools at their disposal, as well. The Commission therefore cannot guarantee that any attacks launched against us will not have an impact.

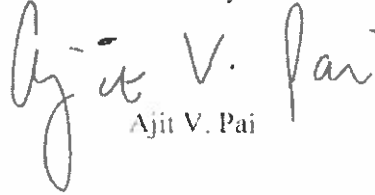
Filers wishing to submit comments to the FCC have four alternatives. They can file using the normal web interface. They can file through the API. They can submit comments using the electronic inbox and the Restoring Internet ECFS Bulk Upload Template. And they can submit a written comment. Should any of these methods be temporarily disrupted or unavailable, members of the public can use an alternative method or wait until the incident has ended. Given the length of time that the Commission has provided for public comment (90 days) as well as the multiple avenues available for submitting such comments, everyone seeking to

Page 2—The Honorable Brian Schatz

participate in this proceeding will have a chance to make his or her voice heard on this important subject.

I appreciate your interest in this matter.

Sincerely,

  
Ajit V. Pai

# Appendix D





Federal Communications Commission  
Washington, D.C. 20554

July 19, 2017

Dell Cameron  
Gizmodo Media Group  
2 West 17<sup>th</sup> St, 2<sup>nd</sup> Floor  
New York, NY 10011  
*Via e-mail to foiaquery@gmail.com*

Re: FOIA Control No. 2017-655

Mr. Cameron:

This letter responds to your Freedom of Information Act (FOIA). Your request has been assigned FOIA Control No. 2017-655. Specifically, your request seeks:

1. All communications between employees in the offices of Chairman Ajit Pai and Commissioner Michael O'Rielly concerning the following topics:
  - a. "distributed denial-of-service attack" or "DDoS"
  - b. Public comments to the FCC's comment system regarding net neutrality.
  - c. "astroturfing"
  - d. "spam" sent to the FCC comment system.
  - e. Dr. David Bray's May 8, 2017, statement regarding the alleged DDoS attack.
  - f. Questions from representatives of the news media regarding the alleged DDoS attack and/or the integrity of the FCC's comment system.
2. All calendar entries, visitor logs, or meeting minutes referring or relating to any and all meetings between employees in the offices of Chairman Ajit Pai and Commissioner Michael O'Rielly regarding the FCC's public comment system and/or the alleged DDoS attack.
3. Any and all documents in the offices of Chairman Ajit Pai and Commissioner Michael O'Rielly discussing, referring, or relating to the FCC's comment system and/or the alleged DDoS attack, including all draft or final versions of orders, memoranda, or written views concerning the approach the FCC should take with respect to perceived issues with the comment system.
4. All records referencing a letter by Senators Ron Wyden and Brian Schatz sent to FCC on May 9 concerning the alleged DDoS attack.
5. All documents and communications in the offices of Chairman Ajit Pai and Commissioner Michael O'Rielly relating to the recommendations or views of FCC personnel about how to respond to the alleged DDoS attack and/or questions about the integrity of the FCC's comment system.
6. A copy of any records related to the FCC "analysis" (cited in Dr. Bray's statement) that concluded a DDoS attack had taken place.

Pursuant to section 0.461(g)(1)(i) of the Commission's rules, the date for responding to your request has been extended July 6, 2017, due to a need to search records from multiple offices of the Commission. The deadline was subsequently extended to July 19, 2017.

The Office of the Chairman, the Office of Commissioner O’Rielly, the Office of Legislative Affairs, and the Office of the Managing Director – Information Technology searched for responsive records.

We located approximately 225 pages of records responsive to your request. Of the approximately 225 pages of responsive records located, 16 pages are produced here. The remaining pages are withheld in full due to the reasons discussed below. Additionally, some material on the pages produced has been redacted due to the reasons discussed below.

Records responsive to your request were withheld under FOIA Exemption 4.<sup>1</sup> Exemption 4 protects matters that are “trade secrets and commercial or financial information obtained from a person and privileged or confidential.” These documents consist of trade press articles and other subscription publications that are subject to copyright. We have determined that disclosure is prohibited by law under the Trade Secrets Act, 18 U.S.C. § 1905, or that release would otherwise harm the commercial interests of the companies involved.

Records responsive to your request were withheld or redacted under FOIA Exemption 5.<sup>2</sup> Exemption 5 protects certain inter-agency and intra-agency records that are normally considered privileged in the civil discovery context. Exemption 5 encompasses a deliberative process privilege intended to “prevent injury to the quality of agency decisions.”<sup>3</sup> To fall within the scope of this privilege the agency records must be both predecisional and deliberative.<sup>4</sup> Predecisional records must have been “prepared in order to assist an agency decision maker in arriving at his decision.”<sup>5</sup> Deliberative records must be such that their disclosure “would expose an agency’s decisionmaking process in such a way as to discourage candid discussion within the agency and thereby undermine the agency’s ability to perform its functions.”<sup>6</sup>

These documents include staffing decisions made by Commission supervisors, draft talking points, staff summaries of congressional letters, and policy suggestions from staff. We have determined that it is reasonably foreseeable that disclosure would harm the Commission’s deliberative processes, which Exemption 5 is intended to protect. Release of this information would chill deliberations within the Commission and impede the candid exchange of ideas.

---

<sup>1</sup> 5 U.S.C. § 552(b)(4).

<sup>2</sup> 5 U.S.C. § 552(b)(5).

<sup>3</sup> *NLRB v. Sears Roebuck & Co.*, 421 U.S. 132, 151 (1975).

<sup>4</sup> *Id.* at 151-52.

<sup>5</sup> *Formaldehyde Inst. v. Dep’t of Health and Human Servs.*, 889 F.2d 1118, 1122 (D.C. Cir. 1989); *see also Coastal States Gas Corp. v. Dep’t of Energy*, 617 F.2d 854, 866 (D.C. Cir. 1980) (“In deciding whether a document should be protected by the privilege we look to whether the document is . . . generated before the adoption of an agency policy and whether . . . it reflects the give-and-take of the consultative process. The exemption thus covers recommendations, draft documents, proposals, suggestions, and other subjective documents. . . .”).

<sup>6</sup> *Formaldehyde Inst.*, 889 F.2d at 1122 (quoting *Dudman Commc’ns Corp. v. Dep’t of the Air Force*, 815 F.2d 1565, 1568 (D.C. Cir. 1987)).

Records responsive to your request were withheld or redacted under FOIA Exemption 6.<sup>7</sup> Exemption 6 protects “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” Balancing the public’s right to disclosure against the individual’s right to privacy, we have determined that release of this information would constitute a clearly unwarranted invasion of personal privacy. These redactions consist of non-public contact information. We have determined that the public interest in this information is de minimis, while there is a substantial privacy interest for the affected individuals.

We have determined that it is reasonably foreseeable that disclosure would harm the privacy interest of the persons mentioned in these records, which Exemption 6 is intended to protect.

Records responsive to your request were withheld under Exemption 7(E), which protects “records or information compiled for law enforcement purposes [the production of which] would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk a circumvention of the law.”<sup>8</sup> These documents consisted of discussion of the Commission’s IT infrastructure and countermeasures. It is reasonably foreseeable that this information, if released, would allow adversaries to circumvent the FCC’s protection measures.

We have determined that it is reasonably foreseeable that disclosure would harm the Commission or the Federal government’s law enforcement activities, which Exemption 7 is intended to protect.

Part 6 of your request seeks “A copy of any records related to the FCC ‘analysis’ (cited in Dr. Bray’s statement) that concluded a DDoS attack had taken place.” IT staff have confirmed there are no records responsive to this portion of the request. The analysis referred to stemmed from real time observation and feedback by Commission IT staff and did not result in written documentation.

The FOIA requires that “any reasonably segregable portion of a record” must be released after appropriate application of the Act’s exemptions.<sup>9</sup> The statutory standard requires the release of any portion of a record that is nonexempt and that is “reasonably segregable” from the exempt portion. However, when nonexempt information is “inextricably intertwined” with exempt information, reasonable segregation is not possible.<sup>10</sup> The redactions and/or withholdings made are consistent with our responsibility to determine if any segregable portions can be released. To the extent non-exempt material is not released, it is inextricably intertwined with exempt material.

We are required by both the FOIA and the Commission’s own rules to charge requesters certain fees associated with the costs of searching for, reviewing, and duplicating the sought after information.<sup>11</sup> To calculate the appropriate fee, requesters are classified as: (1)

---

<sup>7</sup> 5 U.S.C. § 552(b)(6).

<sup>8</sup> 5 U.S.C. § 552(b)(7)(E).

<sup>9</sup> 5 U.S.C. § 552(b) (sentence immediately following exemptions).

<sup>10</sup> *Mead Data Cent. Inc. v. Dep’t of the Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977).

<sup>11</sup> See 5 U.S.C. § 552(a)(4)(A), 47 C.F.R. § 0.470.

commercial use requesters; (2) educational requesters, non-commercial scientific organizations, or representatives of the news media; or (3) all other requesters.<sup>12</sup>

Pursuant to section 0.466(a)(5)-(7) of the Commission's rules, you have been classified as category (2), "educational requesters, non-commercial scientific organizations, or representatives of the news media."<sup>13</sup> As an "educational requester, non-commercial scientific organization, or representative of the news media," the Commission assesses charges to recover the cost of reproducing the records requested, excluding the cost of reproducing the first 100 pages. The production in response to your request did not involve more than 100 pages of duplication. Therefore, you will not be charged any fees.

You have requested a fee waiver pursuant to section 0.470(e) of the Commission's rules.<sup>14</sup> As you are not required to pay any fees in relation to your FOIA request, the Office of the General Counsel, which reviews such requests, does not make a determination on your request for a fee waiver.<sup>15</sup>

If you consider this to be a denial of your FOIA request, you may seek review by filing an application for review with the Office of General Counsel. An application for review must be *received* by the Commission within 90 calendar days of the date of this letter.<sup>16</sup> You may file an application for review by mailing the application to Federal Communications Commission, Office of General Counsel, 445 12<sup>th</sup> St SW, Washington, DC 20554, or you may file your application for review electronically by e-mailing it to [FOIA-Appeal@fcc.gov](mailto:FOIA-Appeal@fcc.gov). Please caption the envelope (or subject line, if via e-mail) and the application itself as "Review of Freedom of Information Action."

If you would like to discuss this response before filing an application for review to attempt to resolve your dispute without going through the appeals process, you may contact the Commission's FOIA Public Liaison for assistance at:

FOIA Public Liaison  
Federal Communications Commission, Office of the Managing Director,  
Performance Evaluation and Records Management  
445 12<sup>th</sup> St SW, Washington, DC 20554  
202-418-0440  
[FOIA-Public-Liaison@fcc.gov](mailto:FOIA-Public-Liaison@fcc.gov)

If you are unable to resolve your FOIA dispute through the Commission's FOIA Public Liaison, the Office of Government Information Services (OGIS), the Federal FOIA Ombudsman's office, offers mediation services to help resolve disputes between FOIA requesters and Federal agencies.<sup>17</sup> The contact information for OGIS is:

---

<sup>12</sup> 47 C.F.R. § 0.470.

<sup>13</sup> 47 C.F.R. § 0.466(a)(5)-(7).

<sup>14</sup> 47 C.F.R. § 0.470(e).

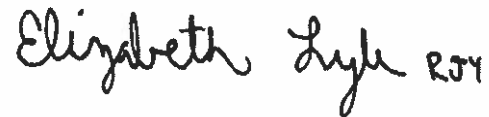
<sup>15</sup> 47 C.F.R. § 0.470(e)(5).

<sup>16</sup> 47 C.F.R. §§ 0.461(j), 1.115; 47 C.F.R. § 1.7 (documents are considered filed with the Commission upon their receipt at the location designated by the Commission).

<sup>17</sup> Please note that attempts to resolve your dispute through the FOIA Public Liaison or OGIS do not toll the time for filing an application for review unless an extension is granted by the Office of General Counsel.

Office of Government Information Services  
National Archives and Records Administration  
8601 Adelphi Road-OGIS  
College Park, MD 20740-6001  
202-741-5770  
877-684-6448  
[ogis@nara.gov](mailto:ogis@nara.gov)  
[ogis.archives.gov](http://ogis.archives.gov)

Sincerely,

A handwritten signature in black ink that reads "Elizabeth Lyle" followed by a small mark that appears to be "RJR".

Elizabeth Lyle  
Assistant General Counsel

Enclosures  
cc: FCC FOIA Office

# Appendix E

**Congress of the United States**  
**Washington, DC 20515**

August 17, 2017

The Honorable Gene Dodaro  
Comptroller General of the United States  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Dodaro:

On May 8, 2017, the Federal Communications Commission (FCC) announced that it was the victim of “multiple distributed denial-of-service (DDos) attacks.” According to FCC staff, these attacks targeted the FCC’s Electronic Comment Filing System (ECFS), the portal through which the public submits comments on ongoing proceedings. More specifically, it appeared that these attacks were designed to disrupt the ECFS during a time period corresponding to the public comment period for the FCC’s *Restoring Internet Freedom Notice of Proposed Rulemaking*, an ongoing proceeding to undo current net neutrality protections.

As you are likely aware, this proceeding has garnered intense public interest. It appears that these attacks were meant to inhibit or limit public comment on this important proceeding, raising doubts about the efficacy of the FCC’s public comment process. Separately, the ECFS has been flooded with fake comments related to the net neutrality proceeding, which undermines this critical component of the FCC’s rule-making process. The FCC’s lack of action in preventing or mitigating this issue is also cause for concern. In fact, taken together, these situations raise serious questions about how the public makes its thoughts known to the FCC and how the FCC develops the record it uses to justify decisions reached by the agency.

While the FCC and the FBI have responded to Congressional inquiries into these DDos attacks, they have not released any records or documentation that would allow for confirmation that an attack occurred, that it was effectively dealt with, and that the FCC has begun to institute measures to thwart future attacks and ensure the security of its systems. As a result, questions remain about the attack itself and more generally about the state of cybersecurity at the FCC – questions that warrant an independent review.

In light of these concerns, we request that the GAO examine the following questions:

1. How did the FCC determine that a cyberattack took place on May 8<sup>th</sup>? What evidence did the security team provide to FCC CIO David Bray before his statement to the press on May 9<sup>th</sup>? What additional evidence did the FCC gather to further support its conclusions after that statement? What documentation did the FCC develop during its investigation of this reported attack, and has it done any after-action reports or other evaluations that would help the FCC respond to future attacks of this nature?

**Congress of the United States**  
**Washington, DC 20515**

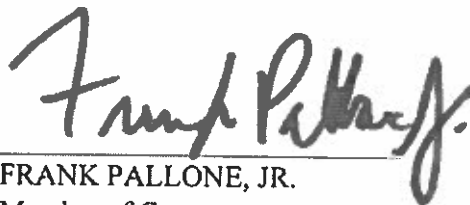
2. What processes and procedures does the FCC have in place to prevent or mitigate a cyberattack on the ECFS like the one that reportedly occurred on May 8<sup>th</sup>? Are these processes in line with best practices and recommendations from the Department of Homeland Security and the National Institute of Standards and Technology? Were these processes followed during and after the May 8<sup>th</sup> attack?
3. The reported May 8<sup>th</sup> attack raises questions about the general vulnerability of the ECFS. Is the ECFS designed in a manner that implements cybersecurity best practices? What are the risks associated with this attack vector? Can other FCC systems be accessed through ECFS vulnerabilities?
4. The attack also raises questions about the security of other FCC's systems. Are the FCC's other public-facing data systems, like the spectrum auction systems, also at risk? Has the FCC evaluated the security of its other public-facing computer systems in light of the reported May 8<sup>th</sup> attack? Has it taken steps to mitigate any vulnerabilities in those systems?

Thank you for your attention to this request. If you have any specific questions, please contact Micaela Klein in Senator Schatz's office at [micaela\\_klein@schatz.senate.gov](mailto:micaela_klein@schatz.senate.gov) or 202-224-3934 and Michael Rogers in Representative Pallone's office at [michael.rogers@mail.house.gov](mailto:michael.rogers@mail.house.gov) or 202-225-4671.

Sincerely,



**BRIAN SCHATZ**  
United States Senator



**FRANK PALLONE, JR.**  
Member of Congress



# Appendix F

---

NEWS > MAY 25, 2017 AT 10:40 EDT

---

## Letter to the FCC from people whose names and addresses were used to submit fake comments against net neutrality

Posted 10:40 EDT on May 25, 2017

May 25, 2017

The Honorable Ajit Pai

Chairman

Federal Communications Commission

445 12th Street, S.W.

Washington, D.C. 20554

Dr. David A. Bray

Chief Information Officer

Federal Communications Commission

445 12th Street, S.W.

Washington, D.C. 20554

CC Members of U.S. Congress

**Dear Chairman Pai,**

Our names and personal information were used to file comments we did not make to the Federal Communications Commission.

We are disturbed by reports that indicate you have no plans [1] to remove these fraudulent comments from the public docket. Whoever is behind this stole our names and addresses, publicly exposed our private information without our permission, and used our identities to file a political statement we did not sign onto. Hundreds of thousands of other Americans may have been victimized too.

**We call on you, the Chairman of the Federal Communications Commission, to take the following actions:**

- Notify all who have been impacted by this attack
- Remove all of the fraudulent comments, including the ones made in our names, from the public docket immediately
- Publicly disclose any information the FCC may have about the group or person behind the 450,000+ fake comments
- Call for an investigation by the appropriate authorities into possible violations of 18 U.S.C. § 1001

As chairman of the FCC, an independent federal agency, it is your responsibility to maintain public trust, especially while your agency is fielding comments on the future of the free and open Internet, an issue that millions of Americans care deeply about.

Based on numerous media reports [2], nearly half a million Americans may have been impacted by whoever impersonated us in a dishonest and deceitful campaign to manufacture false support for your plan to repeal net neutrality protections.

While it may be convenient for you to ignore this, given that it was done in an attempt to support your position, it cannot be the case that the FCC moves forward on such a major public debate without properly investigating this known attack.

All proper authorities must be notified immediately and the FCC must disclose any and all information the agency has pertaining to the organization or person behind these fake comments.

**Sincerely,**

Brittany Ainsworth, Huntington Beach, CA

Greg Baynes, View Park, CA,

William Brahams, San Bernardino, CA

Christian Brown, Redondo Beach, CA

John Burr, New York, NY

Angelica Collins, Bear, DE

Megan Conschafter, Buffalo, NY

Ben Currier, Littleton, CO

Norman Daoust, Cambridge, MA

Cynthia Duby, Desert Hot Springs, CA

Aaron Francis, Santa Ana, CA

Michelle Ellett, Benicia, CA

Adam Galatioto, Gainesville, FL

Surbhi Godsay, Nashua, NH

Daniel Hickey, Worcester, MA

Richard O. Johnson, Castro Valley, CA

Samuel Lewis, Oakland, CA

Paulo Llanes, Seattle, WA

Joel Mullaney, Watertown, MA

Shaun O'Brien, Elito, ME

Nicholas Pannuto, Sterling Heights, MI

Daniel Pinkert, New York City, NY

John Ulick, Champaign, IL

Nicholas Ryan, East Lansing, MI  
Adam Stone, Salt Lake City, UT

[1] <http://www.vocativ.com/431065/fcc-ajit-pai-net-neutrality-bots/>

[2] <https://www.theverge.com/2017/5/10/15610744/anti-net-neutrality-fake-comments-identities>

SHARE ON:

RECENT STORIES:

The FCC sabotaged its own public comments process. Congress needs to stop them from voting to kill net neutrality on December 14

11:03 EST on Nov 30, 2017

Fight for the Future statement on Ajit Pai's ridiculous speech

09:39 EST on Nov 29, 2017

**BREAKING:** First Republican lawmaker to publicly oppose the FCC's radical net neutrality repeal

16:06 EST on Nov 24, 2017



FOLLOW US:

Donate

Shop

Projects

About Us

Contact

News

Branding Guidelines

Major Supporters

Financial Statements

Privacy Policy

Press

How to Support Us

Jobs

Buy a VPN

# Appendix G

GREG WALDEN, OREGON  
CHAIRMAN

FRANK PALLONE, J.R., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (202) 225-2927  
Minority (202) 225-3641

June 28, 2017

The Honorable Jefferson B. Sessions III  
Attorney General  
U.S. Department of Justice  
950 Pennsylvania Ave, NW  
Washington, D.C. 20530

Mr. Andrew G. McCabe  
Acting Director  
Federal Bureau of Investigation  
935 Pennsylvania Avenue, NW  
Washington, D.C. 20530

I write to urge you to investigate whether federal law has been violated by the submission of fake comments to the Federal Communications Commission (FCC) using stolen identities.

This request comes after troubling reports that 14 people recently alerted the FCC that their names and addresses had been used to file net neutrality comments without their knowledge or permission.<sup>1</sup> Reports also indicate that 450,000 identically drafted comments have been filed in the FCC's open internet docket by an unknown party.<sup>2</sup> Other reporting suggests that the persons filing these fake comments may be using information obtained from data breaches.<sup>3</sup>

---

<sup>1</sup> Letter from 14 Persons to FCC Chairman Ajit Pai and FCC CIO David Bray (May 25, 2017) ([www.fightforthefuture.org/news/2017-05-25-letter-to-the-fcc-from-people-whose-names-and/](http://www.fightforthefuture.org/news/2017-05-25-letter-to-the-fcc-from-people-whose-names-and/)).

<sup>2</sup> *People Who Were Impersonated by Anti-Net Neutrality Spammers Blast FCC*, ARS Technica (May 25, 2017) ([arstechnica.com/information-technology/2017/05/identity-theft-victims-ask-fcc-to-clean-up-fake-anti-net-neutrality-comments/](http://arstechnica.com/information-technology/2017/05/identity-theft-victims-ask-fcc-to-clean-up-fake-anti-net-neutrality-comments/)).

<sup>3</sup> *The Anti-Net Neutrality Bot Spamming the FCC is Pulling Names from Leaked Databases*, The Verge (May 11, 2017) ([www.theverge.com/2017/5/11/15626278/net-neutrality-spam-bot-fcc-leak-data](http://www.theverge.com/2017/5/11/15626278/net-neutrality-spam-bot-fcc-leak-data)).

The Honorable Jefferson B. Sessions III  
Mr. Andrew G. McCabe  
June 28, 2017  
Page 2

These parties may be attempting to influence federal policy by publicly misrepresenting the views of innocent victims. As part of its online comment filing system, the FCC is also publicly listing these victims' private information, including their addresses, making this situation more urgent.

Federal law prohibits knowingly making any materially false statement or representation in any matter within the jurisdiction of the executive, legislative, or judicial branch.<sup>4</sup> I am deeply concerned that the sheer number of these potentially false comments suggest a coordinated attempt to materially mislead the FCC, and therefore a coordinated attempt to break federal law. I urge you to take swift action to investigate who may be behind these comments and, if appropriate under applicable federal law and regulations, prosecute the people behind these fraudulent comments.

I appreciate your attention to this important request and ask that you provide me and my staff an update on your progress pursuing this matter one month from today on July 28. If you have any questions, please contact the minority committee staff at (202) 225-3641.

Sincerely,

A handwritten signature in black ink that reads "Frank Pallone, Jr." with a stylized flourish at the end.

Frank Pallone, Jr.  
Ranking Member

---

<sup>4</sup> 18 U.S.C. 1001.