

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK**

-----X

KEVIN COLLIER,	:	
<i>Plaintiff,</i>	:	
- v. -	:	
FEDERAL COMMUNICATIONS COMMISSION,	:	
<i>Defendant.</i>	:	

-----X

COMPLAINT

1. This is an action under the Freedom of Information Act, 5 U.S.C. § 552 (“FOIA”), to order the production of Federal Communications Commission (“FCC”) records concerning public feedback on the agency’s proposed net neutrality rules. Defendant FCC has withheld these records despite proper FOIA requests.

PARTIES

- 2. Plaintiff Kevin Collier (“Collier”) is an investigative journalist whose articles have been read by millions.
- 3. The FCC is an agency of the United States with possession and control of the records sought by Plaintiff.

JURISDICTION AND VENUE

- 4. This court has jurisdiction under 28 U.S.C. § 1331 and 5 U.S.C. § 552(a)(4)(B).
- 5. Plaintiff resides in Brooklyn, New York and therefore venue is appropriate under 5 U.S.C. § 552(a)(4)(B).

FACTS

Hackers and/or Comedian Disables FCC

6. “Net Neutrality” is the principle that internet service providers and governments must treat all data the same, not discriminating or charging differentially by user, content, website, or platform.
7. On April 26, 2017, FCC Chairman Ajit Pai announced plans to roll back Net Neutrality regulations previously promulgated by the agency.
8. On May 7, 2017, comedian John Oliver, the host of HBO's "Last Week Tonight," criticized the Chairman's proposals and encouraged viewers to visit a website with the name “gofccyourself.com.” The site transported users directly to the official FCC page created to receive public comments on the proposal.
9. That evening, the FCC’s website went down, which many attributed to a high volume of pro-neutrality comment traffic inspired by Oliver. However, FCC Chief Information Officer David Bray claimed that the outage was caused by malicious cyber-attacks, known as distributed denial-of-service (or “DDOS”) attacks. (Exhibit A)
10. To date, the FCC has not provided any evidence of a DDOS attack to the public.
11. On May 9, 2017, United States Senators Ron Wyden and Brian Schatz wrote to Chairman Pai requesting further information concerning the alleged DDOS attack and the FCC’s ability to defend against future attacks. (Exhibit B)

Anti-Neutrality Astroturf Comments

12. “Astroturfing” is the practice of creating the illusion of “grassroots” support for policies, providing the false impression of broad popular support.
13. In addition to the many thousands of pro-neutrality comments the agency received, the FCC

has also been flooded with more than 128,000 **identical anti-neutrality** comments. (Exhibit C)

14. Analysis of the comments indicates that many were astroturfed - submitted without the knowledge or consent of the individuals they were attributed to. (Exhibit C)
15. To date, the FCC has not provided any information on whether they believe the comments were part of an astroturf operation or how they intend to determine which, if any, are legitimate.

FOIA Requests and Constructive Denials

16. On May 22, 2017 Collier submitted two FOIA requests to the FCC.
17. The first FOIA request sought records relating to the alleged DDOS attack (the “DDOS Request”).
18. The second FOIA request sought records relating to agency’s analysis of the astroturf anti-neutrality comments (the “Astroturfing Request”).
19. The FCC assigned Collier’s requests tracking numbers “FCC-2017-000661” and “FCC-2017-000662” and granted expedited processing for each on the basis of “urgency to inform the public about an actual or alleged federal government activity.”
20. The records requested are critically necessary to determine whether the FCC is taking appropriate steps to accurately account for public input into its rulemaking.
21. The FCC has provided no responsive records to Collier’s request. By failing to provide - or formally deny - documents within twenty working days, the FBI has constructively denied the request under 5 U.S. Code § 552(a)(6)(A)(ii).

CAUSE OF ACTION

Violation of the Freedom of Information Act for Wrongful Withholding of Agency Records

22. Plaintiff repeats and realleges paragraphs 1-21.
23. Defendant FCC has wrongfully withheld agency records requested by Plaintiff.
24. Plaintiff has exhausted all administrative remedies.

REQUESTED RELIEF

WHEREFORE, Plaintiff requests this Court:

- (A) Order defendant to provide access to the requested documents in their entirety;
- (B) Expedite this proceeding as provided for in 28 U.S.C. § 1657;
- (C) Award plaintiff costs and reasonable attorney fees in this action, as provided in 5 U.S.C. § 552(a)(4)(E); and
- (D) Grant such other and further relief as may deem just and proper.

Dated: July 26, 2017

By: _____



Daniel Novack
NY BAR ID: 5010863
Law Office of Daniel R. Novack
4 New York Plaza (2nd Floor)
New York, NY 10004
Phone: (201) 213-1425
Email: Dan@NovackMediaLaw.com
Counsel for Plaintiff



Media Contact:

Mark Wigfield, (202) 418-0253
mark.wigfield@fcc.gov

For Immediate Release

**FCC CIO STATEMENT ON DISTRIBUTED DENIAL-OF-SERVICE
ATTACKS ON FCC ELECTRONIC COMMENT FILING SYSTEM**

WASHINGTON, May 8, 2017 – Federal Communications Commission Chief Information Officer Dr. David Bray issued the following statement today regarding the cause of delays experienced by consumers recently trying to file comments on the FCC’s Electronic Comment Filing System (ECFS):

“Beginning on Sunday night at midnight, our analysis reveals that the FCC was subject to multiple distributed denial-of-service attacks (DDoS). These were deliberate attempts by external actors to bombard the FCC’s comment system with a high amount of traffic to our commercial cloud host. These actors were not attempting to file comments themselves; rather they made it difficult for legitimate commenters to access and file with the FCC. While the comment system remained up and running the entire time, these DDoS events tied up the servers and prevented them from responding to people attempting to submit comments. We have worked with our commercial partners to address this situation and will continue to monitor developments going forward.”

###

Office of Media Relations: (202) 418-0500
ASL Videophone: (844) 432-2275
TTY: (888) 835-5322
Twitter: @FCC
www.fcc.gov/office-media-relations

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).

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

The Honorable Ajit Pai
Chairman
Federal Communications Commission
445 12th 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 FIR ST
SUITE 201
LA GRANDE, OR 97850
(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

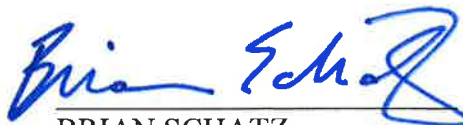
the extent that the FCC utilizes commercial DDoS protection products, did these work as expected? If not, why not?

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



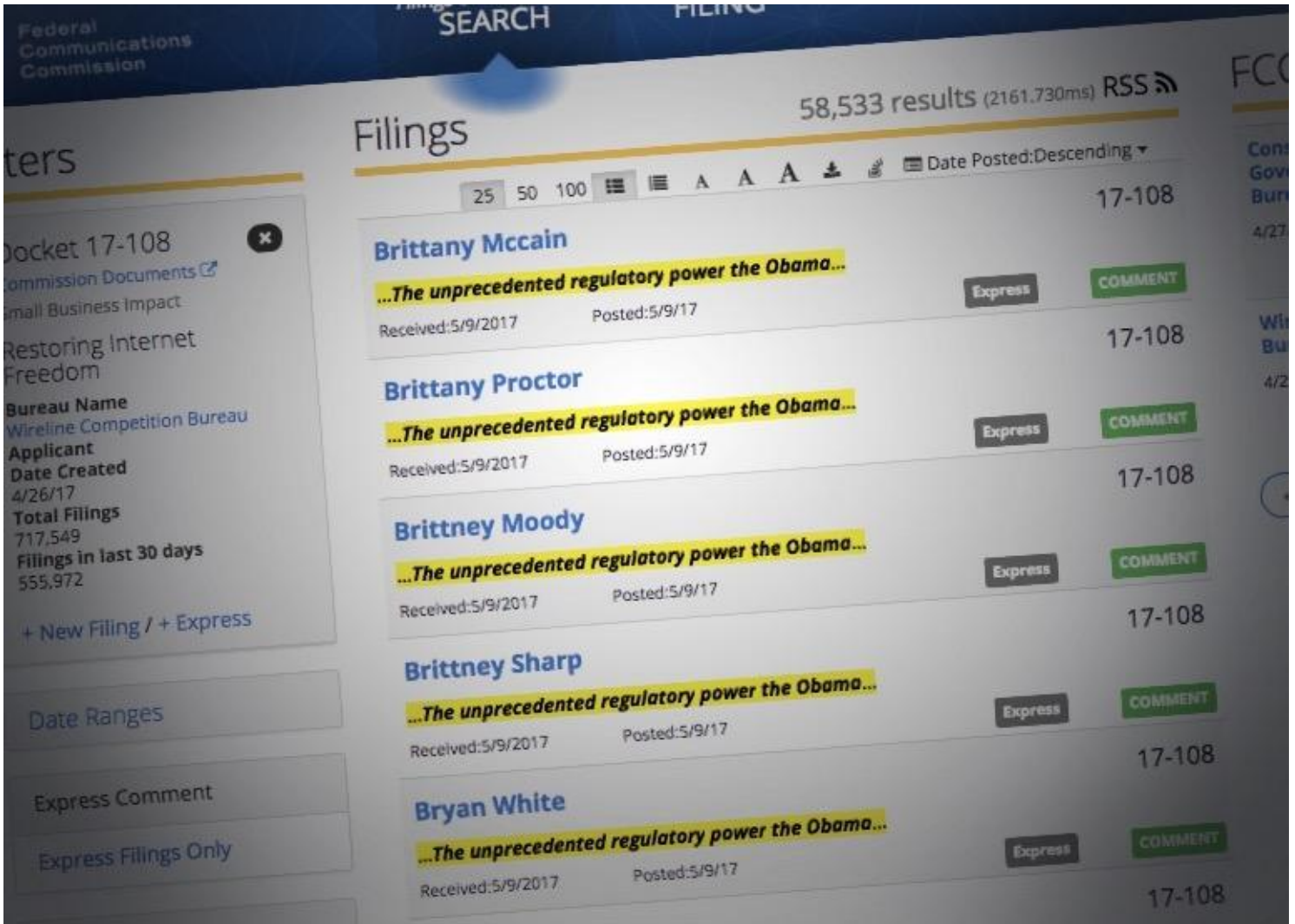
MUST READ SECURITY FLAW IN 3G, 4G LTE NETWORKS LETS HACKERS TRACK PHONE LOCATIONS

Anti-net neutrality spammers are flooding FCC's pages with fake comments

Several people we spoke to denied they had posted comments to the Federal Communication Commission's (FCC) feedback pages.



By Zack Whittaker for Zero Day | May 10, 2017 -- 14:32 GMT (07:32 PDT) | Topic: Security



(Image: file photo)

A bot is thought to be behind the posting of thousands of messages to the FCC's website, in an apparent attempt to influence the results of a public solicitation for feedback on net neutrality.

Late last month, FCC chairman Ajit Pai announced his agency's plans to [roll back an Obama-era framework](http://www.zdnet.com/article/fcc-chairman-launches-process-to-reverse-net-neutrality-rules/) for net neutrality, which rule that internet providers must treat all internet content equally.

Since then, the FCC's public comments system has been flooded with a barrage of comments -- well over half-a-million responses at the time of writing -- in part thanks to comedian John Oliver, who raised the issue on his weekly show on Sunday. He asked Americans to [leave comments](http://www.gofccyourself.com/) in favor of keeping the rules. The FCC later said that it was [hit by "multiple" cyberattacks](http://www.zdnet.com/article/fcc-says-ddos-attacks-not-net-neutrality-comments-tied-up-comments-system/) shortly after the show aired designed to "bombard the FCC's comment system with a high amount of traffic to our commercial cloud host." The FCC, however, offered no evidence of the attacks, with at least one pro-net neutrality group [expressing skepticism](http://tumblr.fightforthefuture.org/post/160454924113/fccs-claim-that-site-was-hacked-during-john) of the FCC's claims.

But a sizable portion of those comments are fake and repeating the same manufactured response.

So much so that [more than 128,000 identical comments](https://www.fcc.gov/ecfs/search/filings?proceedings_name=17-108&q=The%20unprecedented%20regulatory%20power%20the%20Obama%20Administration%20imposed&sort=date_disseminated,DESC)

[108&q=The%20unprecedented%20regulatory%20power%20the%20Obama%20Administration%20imposed&sort=date_disseminated,DESC](https://www.fcc.gov/ecfs/search/filings?proceedings_name=17-108&q=The%20unprecedented%20regulatory%20power%20the%20Obama%20Administration%20imposed&sort=date_disseminated,DESC) have been posted since the feedback doors were opened, now representing a significant slice of the comments on the FCC's feedback docket.

"The unprecedented regulatory power the Obama Administration imposed on the internet is smothering innovation, damaging the American economy and obstructing job creation," the comment says. "I urge the Federal Communications Commission to end the bureaucratic regulatory overreach of the internet known as Title II and restore the bipartisan light-touch regulatory consensus that enabled the internet to flourish for more than 20 years."

The comments follow the same pattern: The bot appears to cycle through names in an alphabetical order, leaving the person's name, postal address, and zip code.

We reached out to two-dozen people by phone, and we left voicemails when nobody picked up. A couple of people late Tuesday called back and confirmed that they had not left any messages on the FCC's website. One of the returning callers specifically said they didn't know what net neutrality was, and a third person reached in a Facebook message Tuesday also confirmed that they had not left any comments on any website.

CNET INTERVIEW



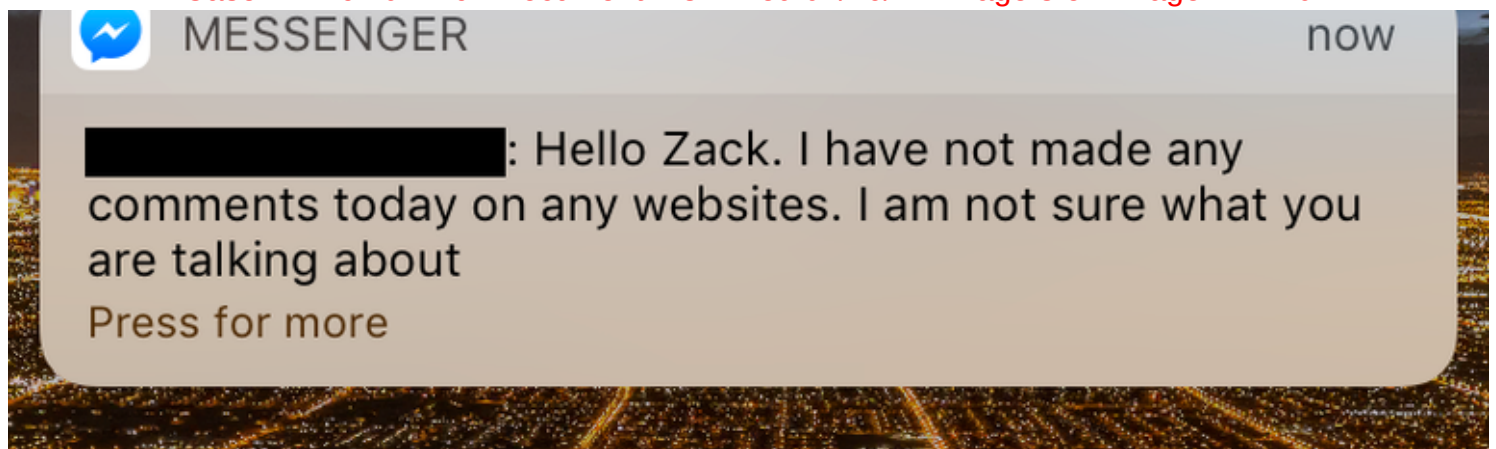
[\(https://www.cnet.com/news/fcc-chair-dishes-on-plan-to-rewrite-net-neutrality-rules/\)](https://www.cnet.com/news/fcc-chair-dishes-on-plan-to-rewrite-net-neutrality-rules/)

FCC chairman's net neutrality fix: 'Clinton-era light touch'

[\(https://www.cnet.com/news/fcc-chair-dishes-on-plan-to-rewrite-net-neutrality-rules/\)](https://www.cnet.com/news/fcc-chair-dishes-on-plan-to-rewrite-net-neutrality-rules/)

Read More

[\(https://www.cnet.com/news/fcc-chair-dishes-on-plan-to-rewrite-net-neutrality-rules/\)](https://www.cnet.com/news/fcc-chair-dishes-on-plan-to-rewrite-net-neutrality-rules/)



(Image: ZDNet)

The bot is likely automatically filing the comments through [the FCC's public comment system API](https://www.fcc.gov/ecfs/public-api-docs.html) (<https://www.fcc.gov/ecfs/public-api-docs.html>), which allows anyone with a free-to-obtain API key to automatically submit comments.

But we don't know where the bot got its names and addresses -- though we suspect it may be from public voter registration records or an older data breach.

We examined individual contribution filings with the Federal Election Commission and found no correlation with names and addresses found on the FCC's comment site. And without email addresses, we weren't able to enumerate entries with breach tools, like [Have I Been Pwned](https://haveibeenpwned.com/) (<https://haveibeenpwned.com/>), to see if there was a common match.

This so-called "astroturfing" technique was first spotted on [several](https://www.reddit.com/r/esist/comments/684oom/public_commenting_on_the_fccs_antinet_neutrality/) (https://www.reddit.com/r/esist/comments/684oom/public_commenting_on_the_fccs_antinet_neutrality/) [different](https://www.reddit.com/r/technology/comments/6a6qvi/someone_is_astroturfing_the_fcc_with_antinet/) (https://www.reddit.com/r/technology/comments/6a6qvi/someone_is_astroturfing_the_fcc_with_antinet/) [threads](https://www.reddit.com/r/technology/comments/6a7i5z/i_keep_seeing_this_really_weird_duplicated/) (https://www.reddit.com/r/technology/comments/6a7i5z/i_keep_seeing_this_really_weird_duplicated/) (and [many more](https://www.reddit.com/r/technology/comments/6aai5n/spammers_are_usurping_the_fcc_filing_comments_for/) (https://www.reddit.com/r/technology/comments/6aai5n/spammers_are_usurping_the_fcc_filing_comments_for/)) on news sharing site Reddit.

But a key question remains: Who's behind the bot?

Several people on those Reddit threads pointed out that part of the bot's comment comes [from a 2010 press release](http://www.prnewswire.com/news-releases/cif-launches-stop-net-regulation-campaign-as-opposition-mounts-to-stop-the-obama-administrations-attempt-to-take-over-the-internet-84705392.html) (<http://www.prnewswire.com/news-releases/cif-launches-stop-net-regulation-campaign-as-opposition-mounts-to-stop-the-obama-administrations-attempt-to-take-over-the-internet-84705392.html>) by the Center for Individual Freedom (CFIF), which vehemently opposes net neutrality in any form. On Wednesday, the group's president Jeff Mazzella confirmed that a "digital media effort that includes a letter campaign" was the source of the block of text, but rejected that CFIF was using bots "in any way, shape or form."

Contact me securely

(<https://medium.com/@zackwhittaker/how-to-contact-me-securely-38dc5c5bc756>)

Zack Whittaker can be reached securely on Signal and WhatsApp at 646-755-8849, and his PGP fingerprint for email is: 4D0E 92F2 E36A EC51 DAAE 5D97 CB8C 15FA EB6C EEA5.

Read More

(<https://medium.com/@zackwhittaker/how->

Mazzella provided a screenshot by email of the email that was sent to its members.

to-contact-me-securely-38dc5c5bc756)

It doesn't mean CFIF is behind the spamming effort. But it doesn't explain how the exact names and addresses of unwitting people were used in the flooding campaign without their permission.

It's also not the first time the FCC's own commenting system has been hijacked to push anti-net neutrality views.

According to a [Vice News report](https://news.vice.com/article/cable-companies-are-astroturfing-fake-consumer-support-to-end-net-neutrality) (<https://news.vice.com/article/cable-companies-are-astroturfing-fake-consumer-support-to-end-net-neutrality>) from 2014, another [anti-net neutrality lobby group](http://www.broadbandforamerica.com/) (<http://www.broadbandforamerica.com/>) working on behalf of the broadband industry hired a public relations firm, the DCI Group, known for its [various astroturfing campaigns](https://thinkprogress.org/exclusive-infamous-astroturf-lobbying-firm-behind-new-anti-health-reform-group-7433df8823c4) (<https://thinkprogress.org/exclusive-infamous-astroturf-lobbying-firm-behind-new-anti-health-reform-group-7433df8823c4>), and was accused of trying to fake consumer opposition to net neutrality.

An email to the DCI Group went unreturned Tuesday. When asked about the supposed bot on its site, a spokesperson for the FCC said the agency does not comment on individual filings.

Comments on the FCC site will be open until mid-August. This case is certainly one we will keep a close eye on.

Updated at 6:10pm: *with comment from CFIF.*

ZDNET INVESTIGATIONS

Leaked TSA documents reveal New York airport's wave of security lapses (<http://www.zdnet.com/article/leaked-files-reveal-catalog-of-airport-security-lapses/>)

US government pushed tech firms to hand over source code (<http://www.zdnet.com/article/us-government-pushed-tech-firms-to-hand-over-source-code/>)

At the US border: Discriminated, detained, searched, interrogated (<http://www.zdnet.com/article/welcome-to-the-united-states-discriminated-detained-searched-interrogated-special-report/>)

Millions of Verizon customer records exposed in security lapse (<http://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/>)

Meet the shadowy tech brokers that deliver your data to the NSA (<http://www.zdnet.com/article/meet-the-shadowy-tech-brokers-that-deliver-your-data-to-the-nsa/>)

Inside the global terror watchlist that secretly shadows millions (<http://www.zdnet.com/article/inside-the-global-terrorism-blacklist-secretly-shadowing-millions-of-suspects/>)

FCC chairman voted to sell your browsing history — so we asked to see his (<http://www.zdnet.com/article/fcc-chairman-browsing-history-freedom-of-information/>)

With a single wiretap order, US authorities listened in on 3.3 million phone calls (<http://www.zdnet.com/article/one-federal-wiretap-order-recorded-millions-phone-calls/>)

198 million Americans hit by 'largest ever' voter records leak (<http://www.zdnet.com/article/security-lapse-exposes-198-million-united-states-voter-records/>)

Britain has passed the 'most extreme surveillance law ever passed in a democracy' (<http://www.zdnet.com/article/snoopers-charter-expansive-new-spying-powers-becomes-law/>)