New York State Office of the Attorney General Letitia James

Fake Comments:

How U.S. Companies & Partisans Hack Democracy to Undermine Your Voice

This report was prepared by the Bureau of Internet and Technology and the Research and Analytics Department, with special thanks to: Assistant Attorney General Noah Stein and Special Enforcement Counsel Jordan Adler, with assistance from Assistant Attorneys General Ezra Sternstein and Hanna Baek, Internet Technology Analyst Joe Graham, and Legal Assistants Richard Borgia and Shirly Huang, all of the Bureau of Internet and Technology, under the supervision of Deputy Bureau Chief Clark Russell and Bureau Chief Kim Berger; Data Scientist Kenneth Morales in the Research and Analytics Department, under the supervision of Deputy Director Megan Thorsfeldt and Director Jonathan Werberg; and Chief Deputy Attorney General Chris D'Angelo. The Office of the New York Attorney General also acknowledges that other law enforcement agencies assisted with the investigation that helped make this report possible.

Contents

Executive Summary

On June 19, 2017, the Federal Communications Commission (FCC) received a comment from Kenneth Langsam of Nassau, New York. Mr. Langsam had written to express support for the proposed repeal of regulations that require internet service providers to treat all internet communications equally. Mr. Langsam "urge[d]" the agency to eliminate these anti-discrimination protections, often referred to as net neutrality rules.

However, there was one problem: Mr. Langsam had died seven years earlier. The comment was fabricated and his identity stolen.

Mr. Langsam's story is not unique; as detailed below, the Office of the New York Attorney General (OAG) found that fake comments accounted for nearly 18 million of the more than 22 million comments the FCC received during its 2017 rulemaking. This type of fraud has significant consequences for our democracy. Federal and state agencies rely on public comments to set standards that govern many aspects of our lives, from public health to consumer protection to the environment, and, in this case, the rules that govern how we share and consume content over the internet. Public comments can also influence legislators and the laws they enact.

This report is the product of an extensive investigation by the OAG of the parties that sought to influence the FCC's 2017 proceeding to repeal the agency's net neutrality rules. In the course of that investigation, the OAG obtained and analyzed tens of thousands of internal emails, planning documents, bank records, invoices, and data comprising hundreds of millions of records. Our investigation confirmed many contemporaneous reports of fraud that dogged that rulemaking process. The OAG found that millions of fake comments were submitted through a secret campaign, funded by the country's largest broadband companies, to manufacture support for the repeal of existing net neutrality rules using lead generators. And millions more were submitted by a 19-year old college student using made-up identities. The OAG also found that the FCC's rulemaking proceeding was not unique. Some of the same parties and tactics have infected other rulemakings and processes for public engagement.

As discussed below, the OAG's investigation resulted in accountability for several of the lead generators who were directly responsible for the submission of fake comments. This office — and other law enforcement agencies — are also continuing to investigate other responsible parties. The OAG has not found evidence, however, that the broadband companies that funded and organized these lead generators had direct knowledge of fraud. Thus, the OAG has not found that they violated New York law. That said, red flags were ignored by the campaign organizers and the way that they conducted their campaign — hiding the broadband industry's involvement, relying on lead generators that used commercial incentives to lure people to comment, and paying dubious vendors for volume rather than quality — is troubling and raises important policy questions.

This report seeks to expose the hidden parties that are responsible for fake comments, the tactics they used, and the harms they caused, so that regulatory agencies and lawmakers can take steps to curb such abuse and provide law enforcement with the tools necessary to hold accountable those who corrupt the democratic process. The report also proposes concrete reforms to enhance accountability and transparency, deter future misconduct, and restore public confidence in the participatory processes that give people a voice in how our government operates.

The following is a summary of the key findings from the OAG's investigation, which are set forth in greater detail in the body of this report:

1. The Broadband Industry's Campaign to Repeal Net Neutrality Rules in 2017 Resulted in Over 8.5 Million Fake Comments to the FCC — Nearly 40% of the FCC's Total — and Over Half a Million Fake Letters to Congress

A. The Broadband Industry Funded a Secret Campaign to Generate Millions of Comments to Provide "Cover" for the FCC's Repeal of Net Neutrality Rules

Internal emails and other documents that the OAG reviewed in its investigation show that, in April 2017, the country's largest broadband companies banded together to fund a campaign to generate millions of comments for the FCC's 2017 net neutrality rulemaking proceeding. The primary funders included an industry trade group and three companies that are among the biggest players in the United States internet, phone, and cable market, with more than 65 million American subscribers among them and a combined market value of approximately half a trillion dollars. The effort was intended to create the appearance of widespread grassroots opposition to existing net neutrality rules, which — as described in an internal campaign planning document — would help provide "cover" for the FCC's proposed repeal. The broadband industry hid its role in the campaign by recruiting anti-regulation advocacy groups, unrelated to the industry, to serve as the campaign's public face. Budget documents show that, in all, the broadband industry players that funded the campaign spent $4.2 million generating and submitting more than 8.5 million fake comments to the FCC.

The broadband industry also sent more than half a million messages to members of Congress purportedly signed by their constituents. Internal emails show that the broadband industry submitted these messages, which voiced support for the FCC's proposal, along with press coverage of the comments the industry had submitted to the FCC, to discourage Congress from interfering with the plan to repeal the rules.

B. The Broadband Industry Engaged Commercial Lead Generators to Manufacture Support for Repeal

The broadband industry could not, in fact, rely on grassroots support for its campaign because the public overwhelmingly supported robust net neutrality rules.[1] So the broadband industry tried to manufacture support for repeal by hiring companies to generate comments for a fee. These companies are known as lead generators. This practice — disguising an orchestrated, paid campaign as a grassroots effort to create a false appearance of genuine, unpaid public support — is often referred to as astroturfing.[2]

The OAG's investigation determined that the bulk of the broadband industry's comments — nearly 80% — were expected to be collected through a type of lead generation known as co-registration. In co-registration, consumers are offered rewards — gift cards, sweepstakes entries, or an e-book of recipes, for example — for providing information about themselves and responding to a series of marketing offers. Marketing offers varied widely, and included everything from discounted children's movies to free trials of male enhancement products, as shown in Figure 1. The broadband industry created solicitations to run alongside these marketing offers, asking consumers to join the campaign opposing net neutrality. Responses would be collected and used to generate comments. The remainder of the comments — roughly 20% — were to be generated using online ads placed on websites across the internet.

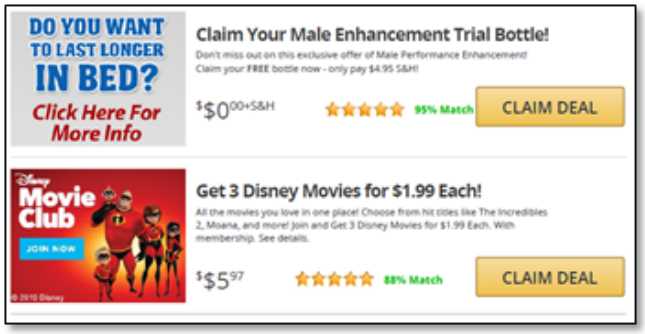


Fig. 1: Example marketing offers from co-registration website used by broadband industry

To conceal the true source of these comments, the broadband industry created webpages for the conservative-leaning advocacy groups through which visitors could submit comments to the FCC supporting repeal. Few comments were submitted through these webpages. But the pages created the impression that comments the FCC received had originated from the advocacy groups' websites and reflected true grassroots support.

Rampant Fraud and Limited Oversight Led to the Submission of More Than 8.5 Million Fake Comments to the FCC and More Than Half a Million Fake Letters to Congress

Nearly every lead generator that was engaged to enroll consumers in the broadband industry's campaign fabricated consumers' responses to the campaign. Most never even ran the broadband industry's campaign solicitation; instead, they copied names and addresses they had purchased or collected months or years earlier through unrelated lead generation efforts, and passed it off as information submitted by consumers who had agreed to join the broadband industry's campaign. One lead generator went a step further, copying information that had been stolen in a data breach and made available online.

In all, six lead generators funded by the broadband industry engaged in fraud. As a result, nearly every comment and message the broadband industry submitted to the FCC and Congress was fake, signed using the names and addresses of millions of individuals without their knowledge or consent.

The OAG has not found evidence that the broadband companies or their lobbying firm had direct knowledge that the lead generators they had funded engaged in fraud. As a result, the OAG has not found that these parties violated New York law. However, the conduct of these broadband companies and their lobbying firm raises serious concerns. These companies hid their involvement in a multi-million-dollar campaign that generated what turned out to be millions of fake comments. The OAG's investigation has demonstrated that the broadband companies' campaign organizers ignored several significant red flags as to the authenticity of the comments that were generated and the integrity of the process. Their limited oversight over the lead generators they had engaged, and the campaign as a whole, provided a fertile environment for lead generators to engage in fraud and deception.

2. The FCC Received Over 9.3 Million Fake Comments Supporting Net Neutrality That Used Fictitious Identities, Most of Which Were Submitted by a 19-Year Old College Student Using Automated Software

A 19-year old college student who opposed the repeal of net neutrality was able to file over 7.7 million pro-neutrality comments with the FCC. Unlike the broadband industry efforts described above that used the names and addresses of real people without their consent, these comments used fabricated names and addresses generated by software. The FCC had few safeguards in place to detect or prevent millions of submissions from a single source. The OAG also identified another group of 1.6 million pro-neutrality comments that were submitted using fictitious identities, but has not determined the source of these comments.

3. Lead Generators' Fraud in Other Advocacy Campaigns Resulted in Millions More Fake Comments, Messages, and Petitions to Government Entities

In the course of its investigation, the OAG found that three of the lead generation firms involved in the broadband industry's net neutrality campaign had also worked on more than 100 other unrelated advocacy campaigns. The firms played the same role in those campaigns: to obtain individuals' consent to submit comments, letters, and petitions to the government. Through this work, the firms helped generate more than 1 million comments for rulemaking proceedings run by the Environmental Protection Agency, the Bureau of Ocean Energy Management, and the FCC, and more than 3.5 million digital signatures for letters and petitions to federal and state legislators and government officials.

The OAG's investigation revealed, however, that nearly all of these comments and messages were fake. The lead generation firms had simply copied names and addresses obtained elsewhere and used them without the individuals' knowledge or consent, just as they had done in the net neutrality campaign.

The OAG has been working with law enforcement partners across the country to hold those involved accountable. Three lead generators have already entered into settlements with the OAG: Fluent, Inc., React2Media, Inc., and Opt-Intelligence, Inc. The settlements require the companies to pay $3.7 million, $550,000, and $150,000 respectively, for their misconduct. The settlements also impose comprehensive reforms for any future campaigns to protect consumers and prevent fraudulent comments. For example, the settlements require robust disclosures to consumers and prohibit the submission of a comment or message to the government on a consumer's behalf in future campaigns unless the consumer has provided express, informed consent. The settlements also require careful monitoring of subcontractors and the retention of records in future campaigns, to ensure appropriate oversight and facilitate investigations into potential misconduct. Further, the settlements require that the companies' role in soliciting comments in future campaigns is disclosed to the government and to the public in any comment docket.

Investigations into others that engaged in fraud are ongoing. But prosecution alone will not be enough. Public participation in government, a bedrock of the nation's democracy, is under assault. The identities of millions of Americans have been misused.

Fraudulent comments and messages, like those submitted by both the broadband industry and the 19-year old student, manipulate rulemaking proceedings and the legislative process by obscuring the popularity of a given policy. Fraudulent comments that also impersonate individuals, like the millions of comments submitted by the broadband industry, compound the harm by subverting individuals' policy preferences and control over their own identities. And astroturfing, of the sort engaged in by the broadband industry, even when it does not involve the type of fraud identified in this report, raises significant policy concerns. Such campaigns by well-funded interest groups can mislead government agencies and officials by creating the false appearance of support from individuals who in fact have not expressed interest in a topic. Moreover, as laid out here, astroturfing can create conditions in which illegal fraud flourishes, incentivizing lead generators that are paid by the lead to cut corners and clients that are focused on goosing volume to dismiss reports of misconduct.

To address these issues, the OAG has several recommendations, described in more detail below: (i) advocacy groups should take steps to ensure that they and their vendors have obtained valid consent from an individual before submitting a comment or message to the government on their behalf; (ii) government agencies and officials that manage electronic systems for receiving comments should hold the advocacy groups and their vendors more accountable for comments they submit, and should implement technical safeguards for bulk submissions using software; and (iii) lawmakers should strengthen laws to deter impersonation and the submission of deceptive and unauthorized comments to the government.

Background

1. Net Neutrality – Purpose and History

Net neutrality refers to the principle that the companies that deliver internet service to your home, business, and mobile phone, such as AT&T, Comcast, and Charter (often referred to as internet service providers, ISPs, or broadband providers), should not discriminate among content on the internet. According to this principle, broadband providers cannot block, slow down, or charge to prioritize certain content; rather, they must treat all content equally. This prevents your broadband provider from acting as a gatekeeper and blocking internet content or applications offered by their competitors or from playing favorites among competing services vying for your attention.

In the absence of strong net neutrality rules, a broadband provider could allow a streaming video service, like the one offered by Netflix, to become degraded for millions of consumers to pressure Netflix to pay the broadband providers more money, or provide preferential treatment to its own streaming TV service over those offered by its competitors.[3]

The FCC, which regulates broadband providers in the United States, first introduced net neutrality protections in 2005. Over the following 10 years, the agency strengthened those protections and addressed new forms of content discrimination by broadband providers. This process eventually resulted in the FCC's 2015 Open Internet Order, which adopted robust, bright-line rules implementing net neutrality principles.

Broadband providers have long opposed strong net neutrality rules, and have fought them in court and through lobbying the FCC and Congress. By contrast, the public has favored net neutrality by wide margins. In 2017, surveys showed the vast majority of Americans across all parties — 75% of Republicans, 89% of Democrats, and 86% of Independents — opposed the repeal of such regulations.[4]

In April 2017, Ajit Pai, as the new chairman of the FCC, initiated a regulatory proceeding to repeal the net neutrality rules established by the agency's 2015 Open Internet Order. Eight months later, in December 2017, the agency released the Restoring Internet Freedom Order, which repealed existing net neutrality regulations.

2. Public Comments – Purposes and Effects

The FCC's 2017 repeal of net neutrality rules was accomplished through a "rulemaking" proceeding, a process by which an agency creates, changes, or repeals a regulation or rule. Federal agencies' rulemaking proceedings must, by law, follow certain steps.[5] Generally, the agency must publish a draft proposal, consider public comments from citizens and stakeholders, and publish a final rule informed by those comments. In some cases, agency leaders must vote to adopt the rule before it can be published. A properly implemented final rule carries the force of law. Many federal agencies engage in rulemaking, including the Environmental Protection Agency (environmental regulations), the Consumer Financial Protection Bureau (financial regulations), and the Securities and Exchange Commission (securities regulations).

Federal agencies accept comments in several ways, including by mail. But the vast majority of comments are submitted through agency-run websites. Some agencies, like the FCC, host their own comments websites. Other agencies use Regulations.gov, a centralized comment collection website managed by the federal government.

Public comments aid agencies in a variety of ways. They provide the public a voice in agency proceedings, giving additional democratic legitimacy for regulations that will govern citizens' lives. They can help identify new facts and surface unanticipated problems with a draft rule. They also help an agency balance competing interests, for example between large corporations and small businesses, or between businesses and consumers.

All of these dynamics played out in the FCC's decision to repeal net neutrality rules in 2017.

3. Comments in the FCC Net Neutrality Proceeding

As soon as the FCC published its proposal to repeal net neutrality rules in April 2017, the agency was flooded with public comments. Researchers quickly found hundreds of thousands of these comments shared identical language.[6] Reporters contacted people whose contact information appeared in suspicious comments, and many of the individuals they reached said they had never seen, much less signed, the comment associated with their name and address.[7] Some had never even heard of net neutrality. Worse, reports confirmed that some "signers" of comments had in fact died before the comment was signed.[8]

By the time the rulemaking proceeding concluded in late 2017, the FCC had received more than 22 million comments, dwarfing the prior record of 3.7 million comments set by the prior FCC net neutrality proceeding in 2015. As described in detail below, the OAG's investigation revealed that nearly 18 million of these comments — the vast majority — were entirely fabricated, and did not reflect people's real viewpoints, with more than 8.5 million of those comments using the names and personal information of real people without their knowledge or consent.

4. A Corruption of the Democratic Process

Fake comments corrupt the democratic process. They cause real harm, enabling monied interests and fraudsters to sway agency rules — undermining public confidence in democratic institutions and robbing citizens of their voice.

First, fake comments twist the regulatory process by obscuring the popularity of a policy. Although rulemaking is not a vote decided based on whichever policy receives the most comments in support, public support can influence the regulations that agencies issue. Indeed, as described below, members of the broadband industry (including a former chairman of the FCC) believed public comments to be so important that their companies spent millions of dollars generating more than 8.5 million comments to, as they put it, provide "cover" to FCC Chairman Pai to repeal net neutrality rules.[9]

Second, fake comments erode public confidence in democratic institutions. When the regulatory process is corrupted, citizens may view the system as rigged or broken, which undermines their faith in the proper working of government. That can further challenge the regulatory process by discouraging participation, leading citizens to believe that submitting a comment is futile because their voice will be drowned out by millions of fakes.

Third, submitting people's names to public comments without their knowledge or consent constitutes impersonation and does real violence to their deeply held beliefs by subverting both their policy preferences and their control over their own identities.

Victims of impersonation in the net neutrality proceeding expressed outrage in complaints they made to the OAG, stating, for example:

» "I'm sick to my stomach knowing that somebody stole my identity and used it to push a viewpoint that I do not hold. This solidifies my stance that in no way can the FCC use the public comments as a means to justify the vote they will hold here shortly."

» "I find it extremely sick and disrespectful to be using my deceased dad to try to make an unpopular decision look the opposite."

» "This is terrifying. Who knows what else has been said falsely under my name?"

» "I am appalled to find my LATE husband's name [] was fraudulently used . . . . My husband passed away last year . . . after a valiant battle with cancer. This unlawful act adds to my pain that someone would violate his good name."

» "I am 72 years old. I don't understand how this happened but I am angry about it . . . people should be held accountable."

» "My 10 year old son's name was used in conju[n]ction with our correct address and his correct email. It appears written by a lobbyist . . . . We feel robbed of our rights . . . ."

» "These are the kinds of actions that make the population lose faith in the system. How many deceased people 'commented' on this? . . . Sickening."

The OAG's Findings

1. The Country's Biggest Broadband Companies Spent $8.2 Million to Oppose Net Neutrality, Including Generating 9 Million Fake Comments and Letters in Opposition

A. The Plan: Manufacture Grassroots Support

In mid-January 2017, several days before Donald Trump was inaugurated as president and set to install a new FCC Chairman, a document was circulated among a small group of senior broadband industry executives laying out a plan to overturn the FCC's existing net neutrality regulations. The document, obtained by the OAG in its investigation, proposed a campaign that would provide support for an anticipated "FCC action to stop the current rule and initiate a new [rulemaking] proceeding."[10] The actions under consideration included financing a campaign to collect and submit a "high-volume [of] comments" to the FCC.[11] The proposed campaign would also urge Congress to pass broadband legislation that would be more permissive than the repealed FCC rules.[12]

Although the FCC did not publicly release a proposal to discard its existing net neutrality rules until April 27, 2017, by early April, the broadband group had already launched a campaign to collect and submit millions of comments to the FCC supporting the agency's as-yet-unannounced plan. The campaign was run through a non-profit organization funded by the broadband industry called Broadband for America ("BFA").[13] BFA's executive committee, made up of senior executives from the broadband companies and trade groups that had contributed to the effort, oversaw the campaign, along with its lobbying firm based in Washington, D.C., which managed the day-to-day operations.[14] BFA hid its role in the campaign by recruiting anti-regulation advocacy groups — unrelated to the broadband industry — to serve as the campaign's public faces.

Planning documents obtained by the OAG show that the goal of the campaign was to manufacture "widespread grassroots support" (a practice often referred to as astroturfing) for the repeal of the FCC's net neutrality regulations.[15] The broadband group believed this support — in conjunction with press outreach, social media campaigns, and coordinated filings from the broadband industry and free-market economists — would "give [FCC Chairman Ajit] Pai volume and intellectual cover" for repeal.[16] Indeed, one broadband industry executive — himself a former chairman of the FCC — advised members of BFA's executive committee, in an email, that "we want to make sure Pai can get those comments in so he can talk about the large number of comments supporting his position."[17]

The BFA executive committee devoted time and significant attention to the volume of comments submitted on both sides of the issue. In emails early on in the campaign, BFA executive committee members expressed concern that the FCC could receive a significant number of comments supporting existing net neutrality rules. Soon after, the lobbying firm began reporting to BFA with great frequency — three times per day — on the number of comments that had been submitted to the FCC.[18] By mid-May, BFA had authorized additional spending to collect more comments opposing net neutrality and discussed plans to adjust the pace of comment submissions to match any increase in pro-neutrality submissions.[19]

By mid-August 2017, BFA's campaign had generated and submitted more than 8.5 million comments to the FCC. To maximize the impact of these comments on the FCC's rulemaking proceeding, BFA commissioned and publicized a third-party study of the comment docket that analyzed the volume of comments favoring repeal of the existing net neutrality regulations.[20] BFA then sent a team to brief FCC staff on the study and provide a tutorial on how they could conduct their own analysis.[21]

BFA's efforts to manufacture support for the repeal of net neutrality went beyond the FCC rulemaking process. BFA simultaneously engaged in a pressure campaign to influence Congress to pass enduring, industry-friendly broadband legislation. In a press release issued in connection with the BFA-commissioned study of FCC comments, BFA urged Congress to take action — stating that the "analysis clearly shows there is strong concern" with the FCC's existing net neutrality regulations.[22] BFA also sent more than half a million letters to members of Congress — voicing support for the FCC's repeal of existing net neutrality regulations and urging Congress to pass broadband legislation favored by the industry.[23]

Budget documents reviewed by the OAG show that, in all, BFA spent approximately $8.2 million on its campaign to repeal the FCC's regulations and push Congress for more favorable law.[24] More than half of that budget — $4.2 million — was used to generate and submit the more than 8.5 million comments to the FCC and the half million letters emailed to Congress.[25] The vast majority of the funding came from three of the nation's largest broadband companies, with one company contributing 47% of the budget and two other companies and a trade group contributing 16% each.[26] Another broadband company and two other trade groups each contributed 1% to 2%.[27]

B. Broadband Company Money Funded Three Astroturfing Efforts, and Each Resulted in Fraud

BFA's efforts to amass millions of comments for the repeal of net neutrality rules proceeded along three parallel tracks, all funded by BFA's industry participants, and coordinated and managed by the lobbying firm that BFA engaged. Each track relied on for-profit "lead generation" firms — businesses that collect names, contact information, and other personal information from consumers and sell that information to third parties — to generate the millions of comments BFA wanted. In each case, the lead-generation companies responsible for getting individuals to sign on to these comments simply resorted to fraud in order to meet their goals.

Two of BFA's three lead-generation efforts relied on "co-registration" sites, which use prizes — such as gift cards or sweepstakes entries — to attract consumers and get them to respond to survey questions and view marketing offers. For the third lead-generation effort, BFA's lobbying firm engaged consultants who promised to collect digital signatures for comments through internet banner ads, exhorting viewers to support the drive to repeal net neutrality rules.

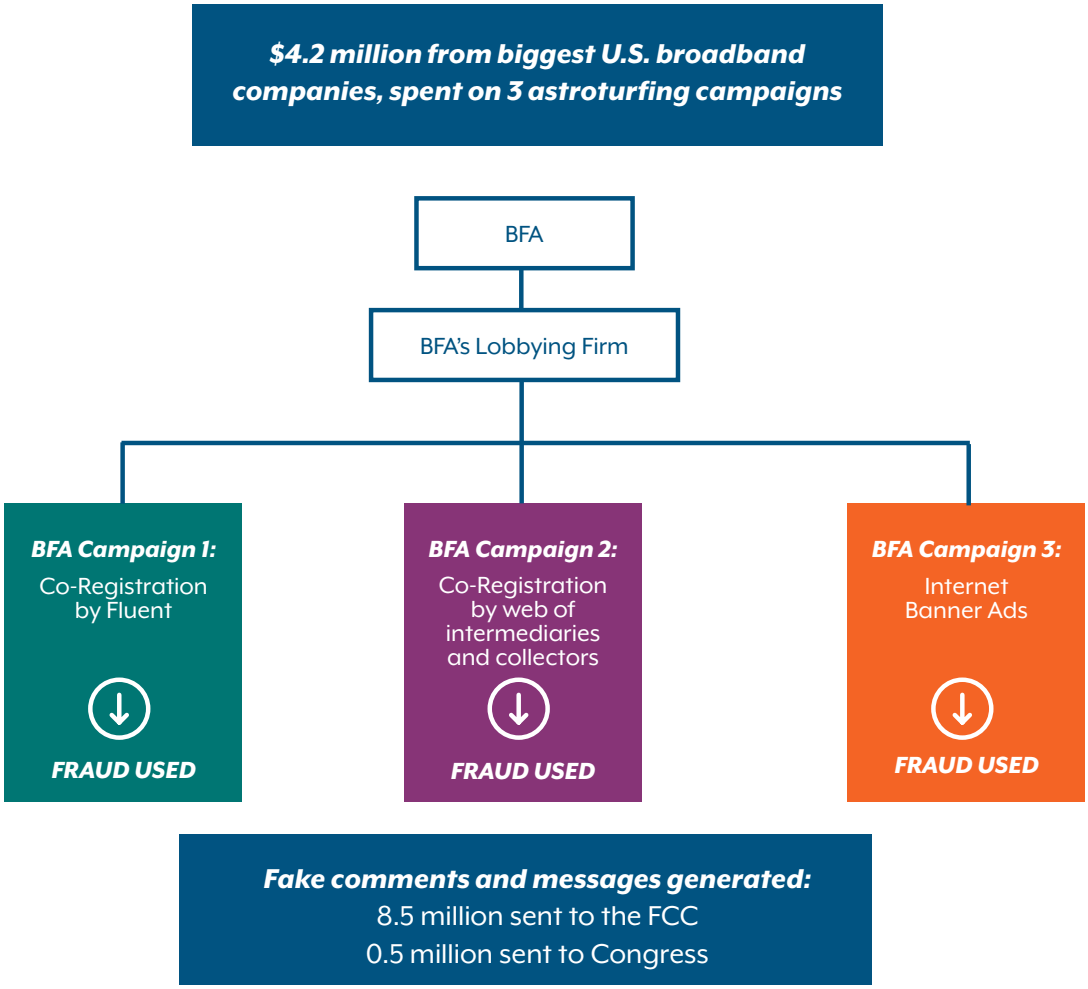
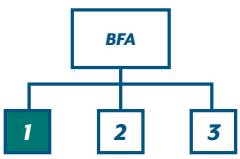


Fig. 2: Overview of BFA's three comment campaigns.



a. BFA Comment Campaign 1: Fraudulent Co-Registration by Fluent

In April 2017, BFA's lobbying firm engaged a New York-based lead generator, Fluent, Inc., to help generate comments for the FCC's net neutrality rulemaking proceeding. BFA ultimately ordered and obtained from Fluent over 5 million digital signatures for its comments, nearly all of which were used in comments submitted to the FCC. However, emails and database records obtained in the OAG's investigation revealed that all of those comments were fraudulent. Fluent never obtained consent from any individuals to submit a comment on their behalf. In fact, it never asked a single person for their consent.

Fluent generates leads through co-registration. Like other co-registration companies, Fluent lures consumers to its co-registration websites with the promise of free prizes, like gift cards, sweepstakes entries, free product samples, and coupons. To claim those prizes, consumers must enter their names and contact information and then view and respond to a series of survey questions and marketing offers. The survey questions typically ask for demographic information and consumption habits. The marketing offers vary but often require that consumers enroll in discounted subscriptions and free trials of products and services.

Figures 3 through 5 are screenshots from the OAG's visit to one of Fluent's co-registration websites during the investigation:

Fig. 3: Homepage displays a prize in exchange for answering survey questions and viewing marketing offers.

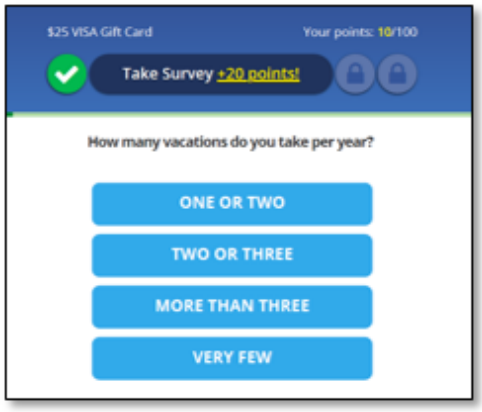


Fig. 4: Survey page displays one of many questions about consumer demographics and spending habits.

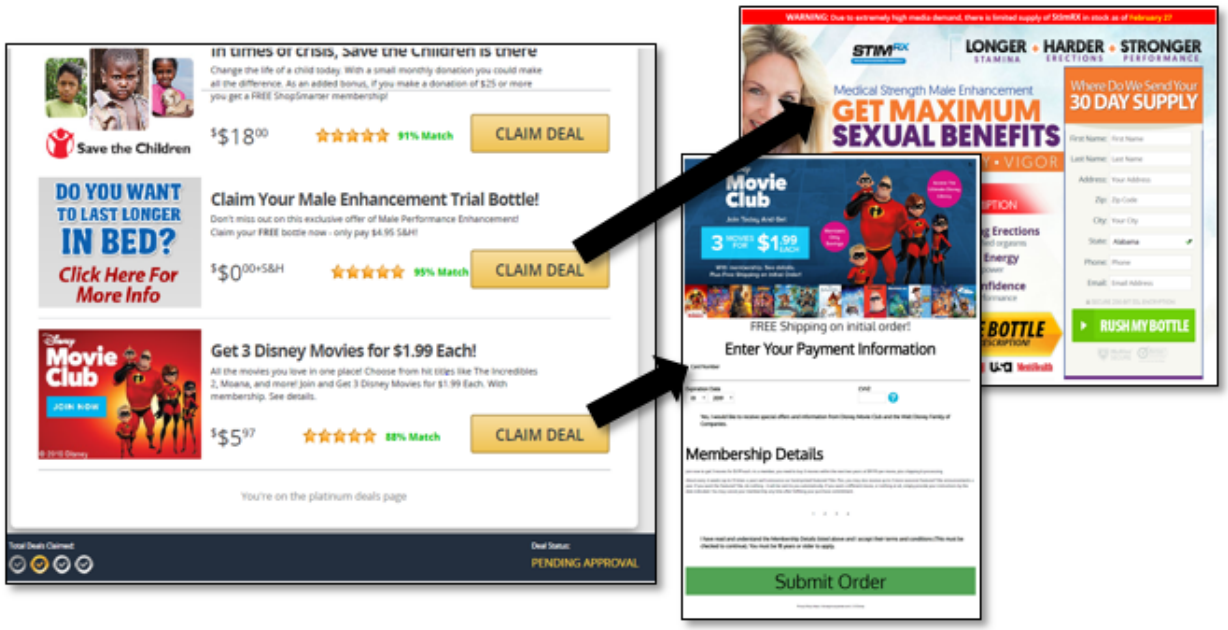


Fig. 5: On the left, an offers page shows "deals" for discounted products or services. Clicking the "CLAIM DEAL" buttons would open windows shown on the right.

In some cases, consumers were required to click through dozens of survey questions and marketing offers before claiming their prize. According to Fluent, hundreds of thousands of consumers registered on its co-registration websites each day.

For BFA's net neutrality campaign, Fluent was hired to place a series of comment solicitations on its co-registration websites to run alongside various commercial marketing offers. Each of these comment solicitations contained a "call to action," asking visitors to submit a comment to the government. For example, one solicitation opened with the following message: "Speak up! Tell the FCC to get their hands off the Internet NOW! Email the FCC now!" Immediately below the call to action were text fields for visitors to enter their names, email addresses, and mailing addresses. Below that was a button by which visitors could consent to the submission of a comment to the FCC on their behalf, and a field containing the text of the comment that would be submitted.

BFA's lobbying firm recruited advocacy groups to "sponsor" these comment solicitations to give the false impression to the public and policymakers that there were a multitude of different voices clamoring for the repeal of the existing net neutrality rules. Using the names of these non-profit sponsors — instead of the name of BFA or its member companies — also had the effect of obscuring the broadband industry's role in orchestrating and funding the effort.[28] The advocacy groups' involvement was largely limited to branding; their names appeared prominently in the solicitations rather than BFA's. Different solicitations were created for each advocacy group, with each solicitation bearing different images and comment text. Figure 6 below depicts a Fluent-created mockup of one such comment solicitation, "sponsored" by the advocacy group Taxpayers Protection Alliance.

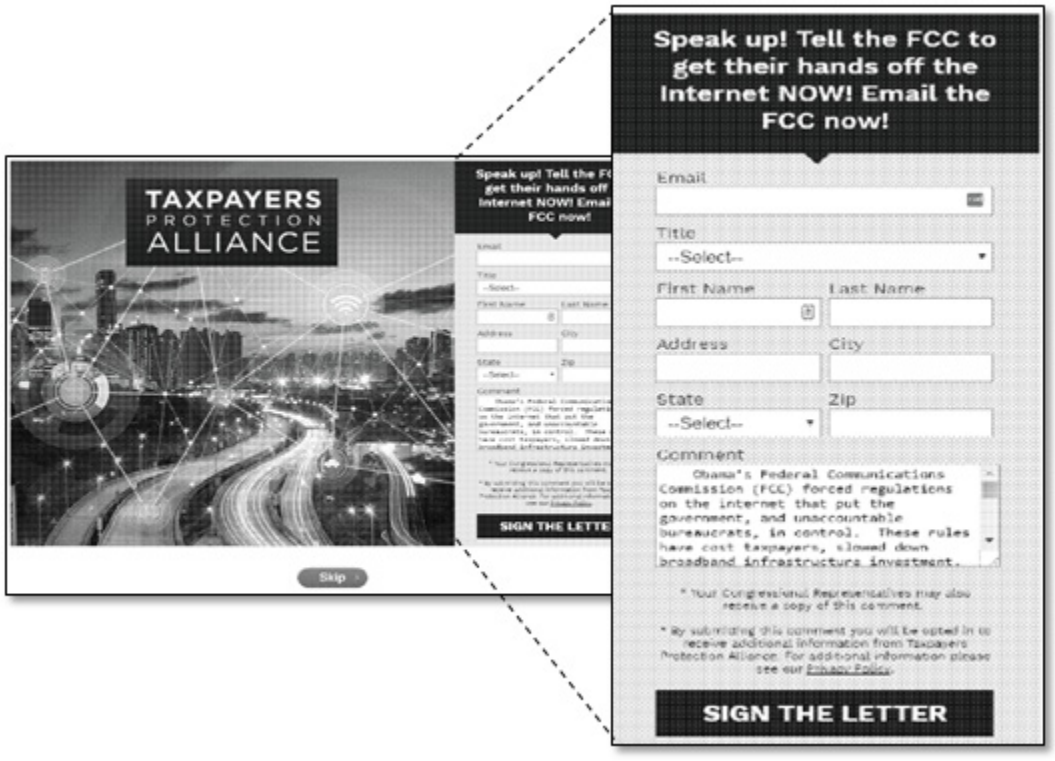


Fig. 6: A mockup of a BFA comment solicitation, sponsored by the non-profit Taxpayers Protection Alliance, that Fluent presented to BFA's lobbying firm for approval to place on Fluent's co-registration website.

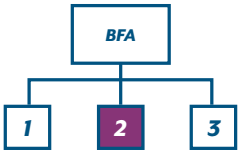
Contrary to its representations to BFA's lobbying firm, Fluent never ran any comment solicitations on its websites, and, accordingly, never obtained anyone's consent to submit comments to the FCC. Instead, Fluent copied information consumers had provided when registering on one of Fluent's websites — in some cases, months or years earlier — and passed it off as personal information entered into the comment solicitation by individuals who had agreed to participate in the campaign to repeal net neutrality rules.

BFA's net neutrality comment campaign with Fluent ran on and off from May 8 through August 15, 2017. At the conclusion of the campaign, Fluent falsely claimed that the campaign had yielded comments from more than 5 million consumers. In fact, none of those 5 million people had been shown the comment solicitations, much less consented to have those comments submitted to the FCC on their behalf. Nevertheless, Fluent transferred these individuals' names and contact information to a third party that BFA's lobbying firm had hired, to submit the comments to the FCC on BFA's behalf. The OAG determined that the third party ultimately submitted 4.69 million comments to the FCC based on the information Fluent provided.

Fluent's conduct attracted notice. Several individuals discovered their names and addresses had been used in messages to the government that they had not seen or authorized. The individuals were angry and they complained about the impersonation.

Their complaints were forwarded to BFA's lobbying firm, which presented them to Fluent with a request for an explanation. Fluent responded to the inquiries with misrepresentations, falsely stating that the consumers had indeed been shown the full text of the comment and had expressly authorized its submission. To support its misrepresentations, Fluent provided data purporting to prove that consumers had agreed to the comment, including a date and time when the consumer had supposedly viewed the solicitation.

To further conceal the scheme from its client, Fluent used what it referred to as "show-me sites." Show-me sites looked like Fluent's typical co-registration sites. However, unlike the typical co-registration sites, show-me sites did not have any live traffic and were not used to collect leads. Instead, the sites were used to stage offers for clients seeking confirmation that their campaigns were live and offers were being displayed correctly. Fluent would falsely represent to these clients that the sites, and the offers on the sites, were live. For example, before one call with BFA's lobbying firm, a Fluent employee hurriedly asked a colleague to post one of the net neutrality comment solicitations on a show-me site, writing "I have to jump on a call with [the client] to prove our process is legit this morning. Just to be on the safe side I need someone to throw up one of these [solicitations] . . . on SamplesandSavings [a show-me site]."



b. BFA Comment Campaign 2: Fraudulent Co-Registration by a Web of Intermediaries and Collectors

In March 2017, BFA's lobbying firm also engaged a Washington, D.C.-based firm for a second campaign to generate an additional 2 million comments supporting the repeal of existing net neutrality rules. Emails, invoices and database records the OAG obtained revealed that the work was parceled out through a web of contractors and subcontractors to several co-registration firms, which were directed to solicit consumers to participate in the campaign.[29] These co-registration companies ultimately supplied the names and contact information of over 2 million people who they claimed had consented to the submission of a comment to the FCC on their behalf. In reality, five of these co-registration companies, responsible for 96% of the total, fabricated all or nearly all of the records of consent they had provided — 1.99 million records out of 2.07 million. To do so, they used personal information purchased from other lead generators or gathered from consumers months or years earlier in unrelated co-registration campaigns.

The Washington, D.C.-based firm hired by BFA's lobbying firm subcontracted the work to Opt-Intelligence, a small New York-based co-registration company. Opt-Intelligence collected few, if any, comments itself, and, instead, further subcontracted the work out to two other co-registration businesses. One of those subcontractors did not itself collect comments, but instead engaged three additional co-registration businesses to perform the work, one of which in turn engaged ***still other*** co-registration businesses. Figure 7 illustrates this web of entities.[30]

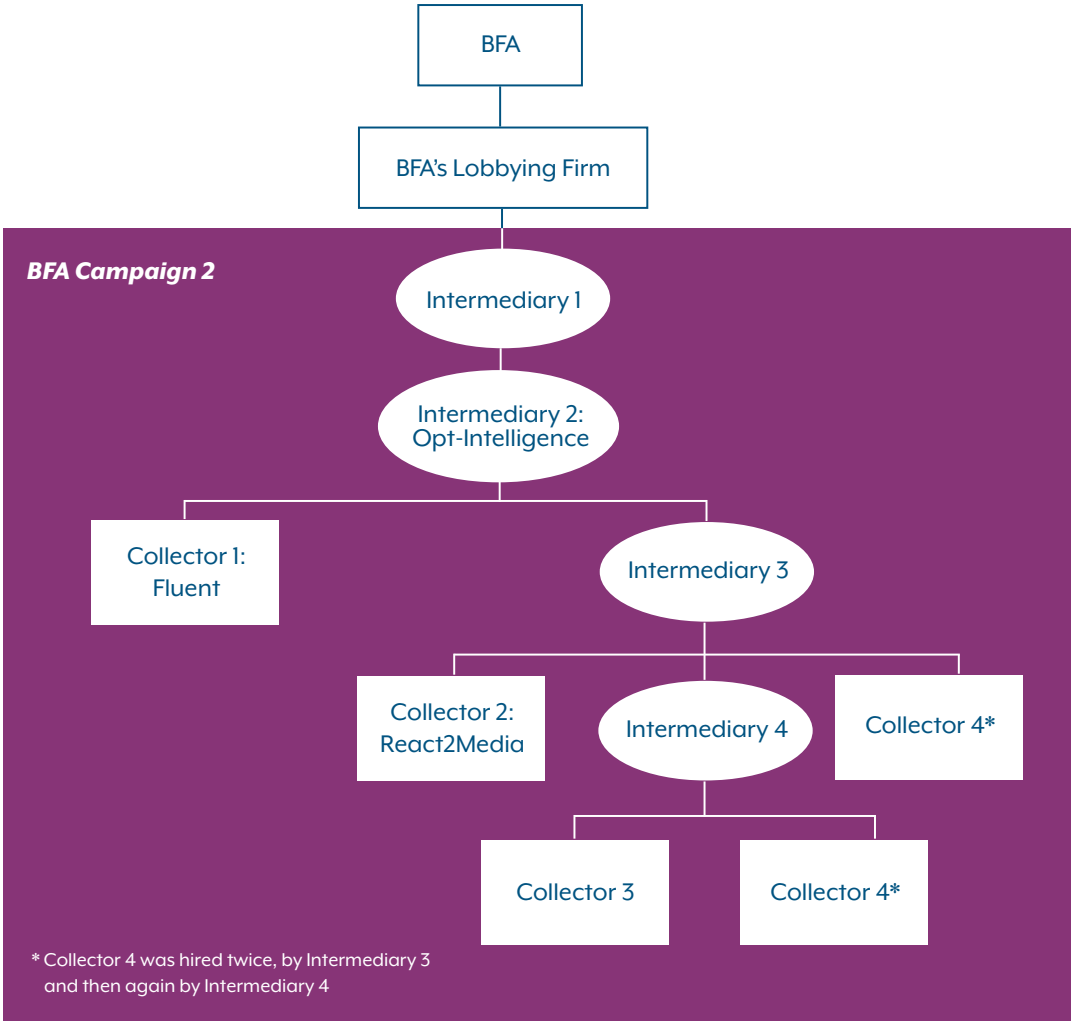


Fig. 7: Convoluted supply chain of co-registration companies that provided comments for BFA's Campaign 2.

Several of these companies acted solely as go-betweens. At the outset, each company received campaign specifications from its client — the intermediary directly above it in the chain shown in Figure 7 — with the language and images it would need to present to users. The company then passed those campaign specifications to its subcontractors. As subcontractors delivered names and contact information of individuals who had ostensibly agreed to participate in the campaign, the intermediaries performed some minimal processing of the data, such as weeding out duplicates and then delivering the information to their own clients immediately above them in the chain.

Each of these intermediaries kept a portion of BFA's payment for itself. As a result, several of the companies at the bottom of the chain — which ostensibly bore the cost of operating co-registration websites and purchasing traffic to those sites — were paid only $0.03 or $0.04 per comment. One co-registration firm told the OAG that it would not have been possible to run a legitimate co-registration campaign that was profitable at that price point.

This arrangement created an environment that was ripe for fraud. The layers of intermediaries separating BFA's lobbying firm at the top of the web from the co-registration firms at the bottom of the web made those co-registration firms unaccountable. Indeed, none of these companies, including those at the top, were aware of the complex web of contractors and sub-subcontractors involved in the campaign. Most knew of only those companies with which they had direct contact.

Like Fluent, the companies further down the chain operated co-registration websites that offered incentives to individuals who agreed to provide their personal information to marketers. Individuals were promised, among others things, "free cash," gift cards, product "samples," and even an e-book of chicken recipes.

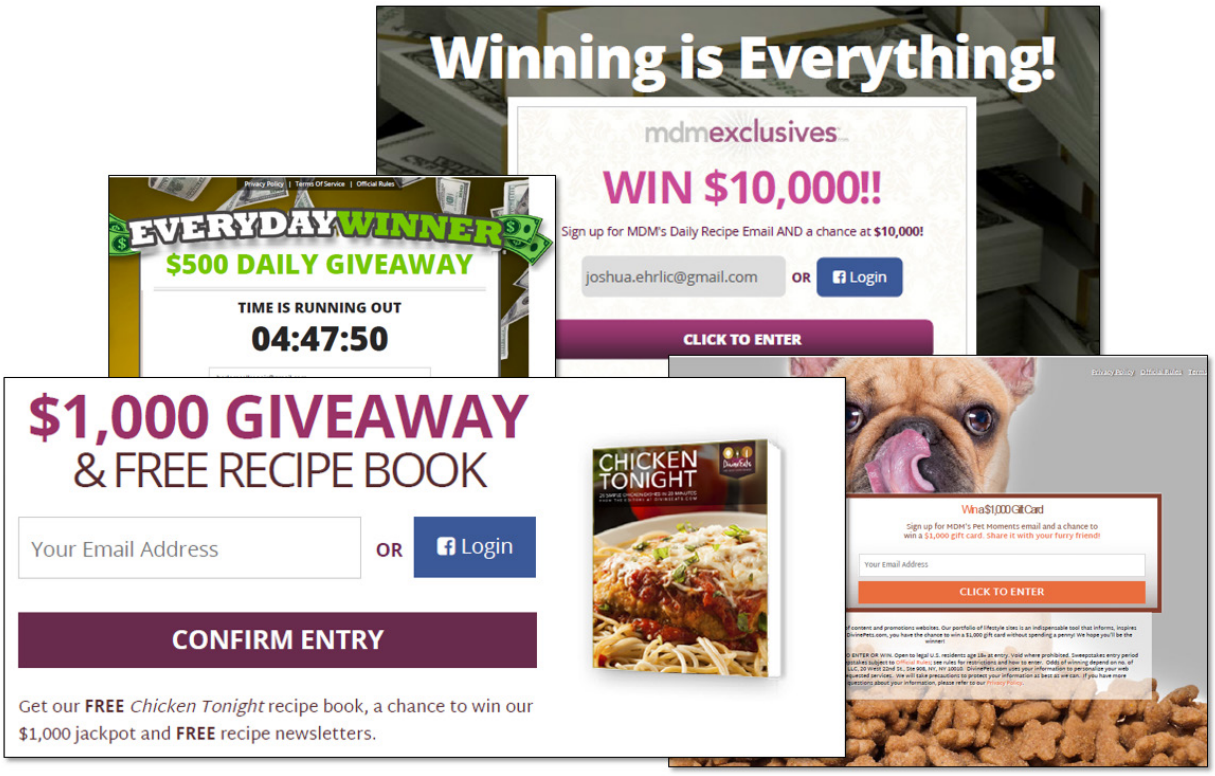


Fig. 8: Screenshots showing prizes used to lure consumers to sites of a co-registration company.

Each of these co-registration companies was provided with a comment solicitation that could run alongside marketing offers and was to be used to obtain individuals' consent for the submission of a comment to the FCC on their behalf. The solicitation was similar to those Fluent was instructed to use in Comment Campaign 1, described above, but featured a different sponsor and comment text. One mockup of the comment solicitation is shown in Figure 9 below.

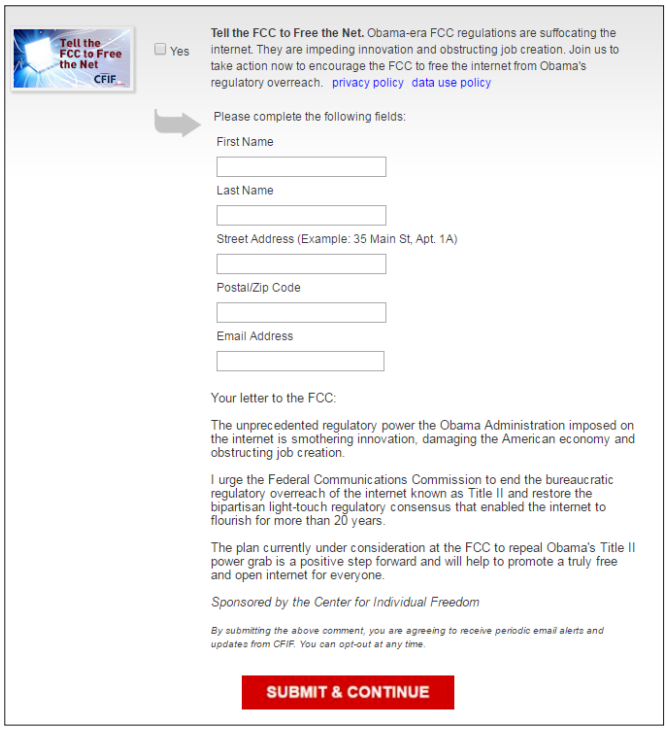


Fig. 9: Mockup of a BFA comment solicitation that a co-registration company presented for approval to place on its website.

When the campaign concluded, the co-registration companies had provided BFA's lobbying firm with names and contact information of more than 2 million consumers who had purportedly agreed to participate in the comment campaign.

In fact, few, if any of these individuals had consented to the submission of comments to the FCC on their behalf. Over the course of its investigation, the OAG painstakingly traced these comments through the chain of co-registration companies back to their sources — ultimately identifying five companies that were responsible for approximately 1.99 million of 2.07 million comments, or 96% of the total.[31] The OAG found that all five of these co-registration companies generated all or nearly all of their comments through outright fraud; instead of showing a comment solicitation, they had simply fabricated consent for the individuals they said they had reached. The owner of one company admitted to the OAG that his company did not even operate a co-registration website at the time; the company had shuttered the site approximately seven years earlier.

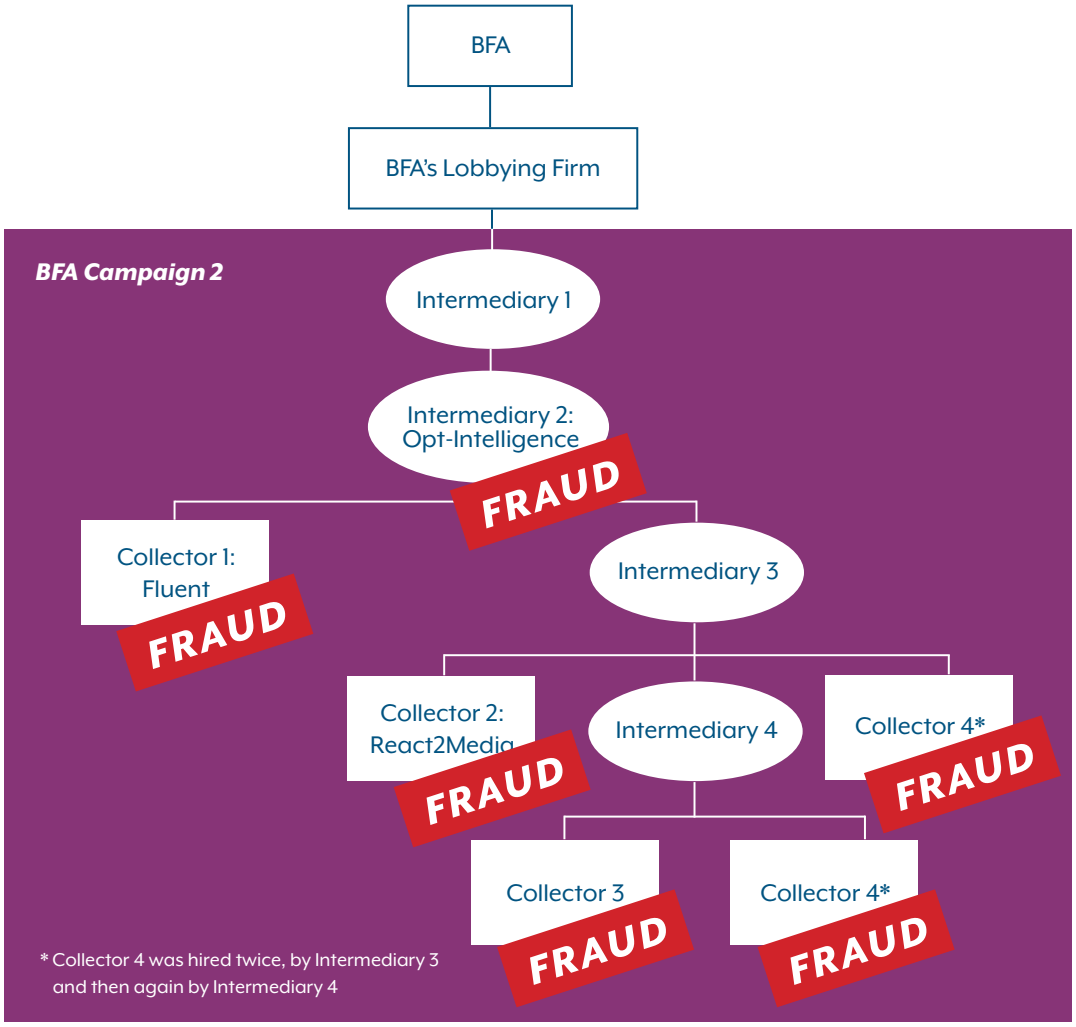
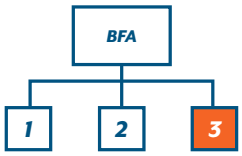


Fig. 10: Multiple co-registration companies, responsible for 96% of the comments in BFA's Campaign 2, engaged in fraud.

The companies created these records by copying old data — names and contact information — they had compiled for other campaigns or purchased from other lead generators. To conceal that the information had been copied without individuals' consent, the companies generated false timestamps for each record that purportedly reflected the time each individual had viewed the campaign and agreed to participate. The timestamps were generated at varying intervals over the course of the day, to avoid the appearance that they were artificial. Notably, although the companies' methods were similar, each of these five companies acted independently, unaware that there were other companies involved in the campaign that were also committing fraud.



c. BFA Comment Campaign 3: Fraudulent Internet Banner Ads

In May 2017, BFA launched a third campaign to collect approximately 1.5 million comments using internet banner ads. These ads — running on a variety of websites like people.com, economist.com, and dailycaller.com — would ask visitors to join a comment campaign to the FCC from within the ads themselves. However, emails and database records obtained in the OAG's investigation revealed that the company engaged to run the ads ran few, if any. Instead, it fabricated all or nearly all of the more than 1.5 million records of consent it claimed to have obtained. The personal information that commenters had purportedly entered had, in fact, merely been copied from other sources, including records that had been stolen in a data breach and dumped online.

To oversee this campaign, BFA hired the Georgia-based firm of a well-connected and influential political consultant, which in turn hired a small Virginia-based company. Both the Georgia-based firm and the Virginia-based firm sold consulting services to corporate clients and advocacy groups for, among other things, public comment campaigns. The Virginia firm engaged a small California-based digital advertising company, which claimed to have a novel way of signing up individuals using online advertising. The advertising company claimed it could place advertisements for the comment campaign on websites across the internet and then collect individuals' names, contact information, and consent to submit a comment to the FCC on their behalf, using text entry fields within the advertisement itself.

The advertising company provided the Virginia-based company with mockups of the advertisement, shown in Figure 11 below. The first panel of Figure 11 depicts the advertisement as it would appear when a user first loaded a webpage. If an individual clicked on the advertisement, the individual would then be asked to enter their name, email address, and address into several small text fields ***within*** the advertisement. If the individual entered this information and clicked on the button labeled "Submit," the message in the third panel thanking them for their submission would replace the text fields. The advertising company claimed that it would collect all of these submissions and then provide them to the Virginia-based company to submit to the FCC.

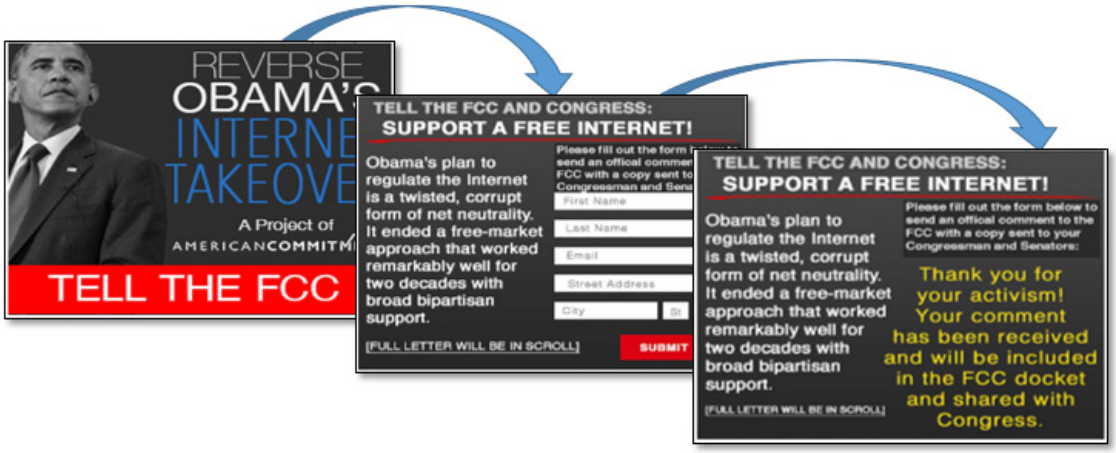


Fig. 11: Mockups the digital advertising company created in advance of the campaign, illustrating its claimed ability to capture user information within a banner ad.

The companies were acutely aware that the submission of a large volume of identical comments could attract scrutiny, such as from the press, researchers, and pro–net neutrality advocacy groups. As a result, they used two tactics to obscure the fact that the comments they generated had originated from a single source.

First, the advertising company used software to create unique text for each comment. A template was created, akin to a Mad Libs, with blank fields that would be populated with a word or phrase chosen at random from a predefined pool. For example, the template opened with a blank field that would be filled in with one of the following:

> "Dear FCC,"; "Mr. Pai:"; "Dear Mr. Pai,"; "Dear Chairman Pai,"; "Chairman Pai:"; "To whom it may concern:"; "FCC commissioners,"; "FCC:"; "Dear Commissioners:"; "To the Federal Communications Commission:"; "To the FCC:";

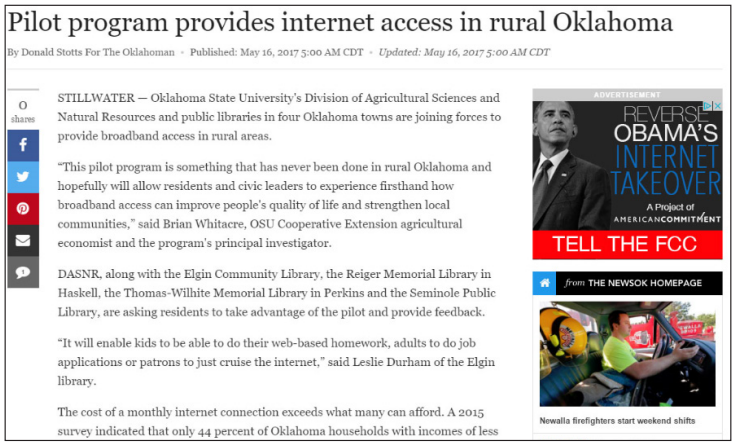
The template contained 35 of these Mad Libs-style blank fields, each of which had between 2 and 30 words or phrases that could be used. After reviewing the plans, an executive of the Georgia-based firm that BFA had hired to oversee the effort remarked on the number of possible combinations:

> "I'm no math major, but I count . . . [n]early 24 decillion permutations. The NSA could handle it, but I doubt [the pro–net neutrality advocacy group] Public Knowledge could."

The digital advertising firm generated more than 1 million comments in this manner.

Second, in addition to the Mad Libs–style comments, the digital advertising firm was instructed to use five static comment texts. The campaign sponsor explained in email that this would create the "appearance of multiple, unrelated efforts" to collect comments by five unrelated organizations. An employee of the digital advertising firm agreed, stating that "it would be hard to pin point where [the comments] are coming from." These five static comment texts were used to generate hundreds of thousands of additional comments.

The advertising company reported that its ads ran from May 12, 2017 to May 18, 2017, and appeared on dozens of high-traffic websites, including yahoo.com, economist.com, breitbart.com, and dailycaller.com. The company sent screenshots of sites where it claimed the ad had run to the Virginia-based firm helping to oversee the campaign.


Pilot program provides internet access in rural Oklahoma

By Donald Stotts For The Oklahoman · Published: May 16, 2017 5:00 AM CDT · *Updated: May 16, 2017 5:00 AM CDT*

0 shares

STILLWATER — Oklahoma State University's Division of Agricultural Sciences and Natural Resources and public libraries in four Oklahoma towns are joining forces to provide broadband access in rural areas.

"This pilot program is something that has never been done in rural Oklahoma and hopefully will allow residents and civic leaders to experience firsthand how broadband access can improve people's quality of life and strengthen local communities," said Brian Whitacre, OSU Cooperative Extension agricultural economist and the program's principal investigator.

DASNR, along with the Elgin Community Library, the Reiger Memorial Library in Haskell, the Thomas-Wilhite Memorial Library in Perkins and the Seminole Public Library, are asking residents to take advantage of the pilot and provide feedback.

"It will enable kids to be able to do their web-based homework, adults to do job applications or patrons to just cruise the internet," said Leslie Durham of the Elgin library.

The cost of a monthly internet connection exceeds what many can afford. A 2015 survey indicated that only 44 percent of Oklahoma households with incomes of less

ADVERTISEMENT

REVERSE OBAMA'S INTERNET TAKEOVER

A Project of AMERICANCOMMITMENT

TELL THE FCC

from THE NEWSOK HOMEPAGE

Newalla firefighters start weekend shifts

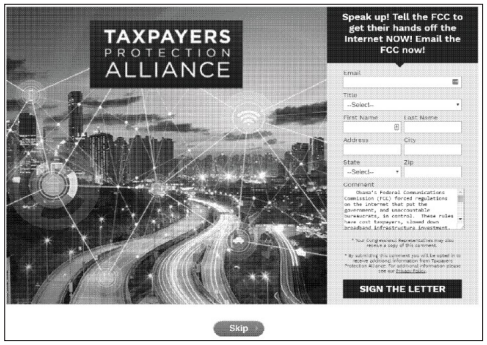
Fig. 12: An example of a screenshot that the advertising company sent, purporting to show the placement of the advertisement.

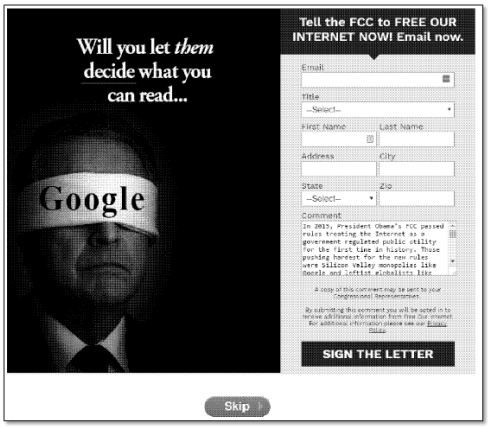
The advertising company claimed that during this seven-day period, more than 1.5 million people entered their personal information into the text boxes in the advertisement and agreed to have comments submitted to the FCC on their behalf. In fact, none of these people had done so. The advertising company had simply copied the names and contact information of approximately 1.4 million people from records that had been stolen in a data breach and dumped online in 2016.[32] For most of the remaining comments — approximately 100,000 — the advertising company brazenly copied information it had provided to the Virginia-based company just a year earlier for comments in a different FCC regulatory proceeding.[33]

Although the advertising company had provided records for 1.5 million people, when the comments were submitted to the FCC several hundred thousand comments were submitted twice. As a result, more than 1.85 million fake comments were submitted to the FCC based on the advertising company's work.

C. The Broadband Industry Hid Its Involvement Behind Advocacy Groups to Create the False Impression of Widespread Grassroots Opposition to Net Neutrality

BFA went to great lengths to create the false impression that the millions of anti–net neutrality comments it had funded reflected widespread grassroots opposition to existing net neutrality rules. Emails that the OAG obtained show that, at the outset, BFA engaged several non-profit advocacy organizations to act as fronts for its campaign. Every comment solicitation and advertisement that BFA and its lobbying firm directed the vendors to run were "sponsored" by and prominently featured the name of one of these advocacy organizations: American Commitment, the Center for Individual Freedoms, the Taxpayers Protection Alliance, and Free Our Internet. Neither BFA, nor its broadband industry benefactors, were identified anywhere. Emails among BFA's lobbying firm and BFA's executive committee, as well as from the lobbying firm to the vendors, reveal that, behind the scenes, BFA maintained control over virtually every aspect of the campaigns.





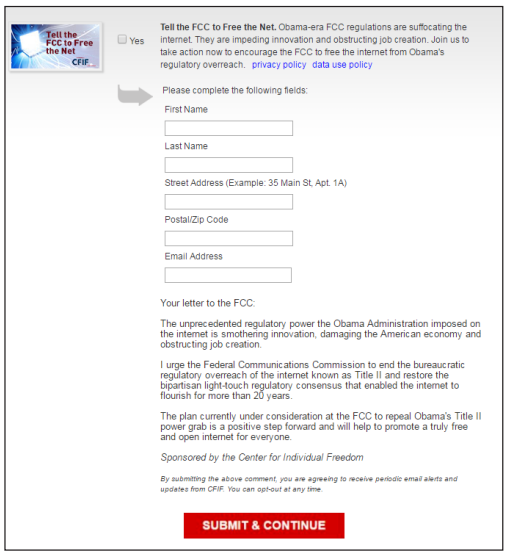


Fig. 13: Mockups prepared using names and logos of three advocacy group "sponsors," for use on co-registration sites.

This effort was deliberately structured to create the false impression that the comments were generated through independent campaigns run by a variety of different organizations. In addition to engaging multiple advocacy groups as "sponsors," as described above, one of BFA's advocacy groups rotated through five distinct comment texts. The head of the advocacy group explained why in an email exchange with a vendor:

> Advocacy group head: "[We're] [i]nterested in [the] appearance of multiple, unrelated efforts."
>
> Vendor: "I think I understand . . . there could be 5 or 6 different organizations like American Commitment leading a comment charge on against ***[sic]*** the Obama administration net neutrality rules. Is that correct?"
>
> Advocacy group head: "Correct."

BFA reinforced the misimpression it had sought to cultivate — that comments reflected grassroots support by individuals engaged in the issue — by concealing how the comments were generated. Records obtained by the OAG show that BFA's lobbying firm engaged vendors to help create webpages for the advocacy organizations' websites that could be used to solicit and collect comments.[34] The pages were similar to the comment solicitations and ads that lead generators were directed to run: they contained fields a visitor could use to enter their name and contact information, and a text box with pre-written comment text identical to the comment text used in the lead generation campaigns. Few, if any, comments were actually collected through these pages. But they were useful as decoys — anyone who tried to identify the source of BFA's comments would inevitably connect them to the advocacy group's public website and not the hidden lead generation pages where they were actually generated.

BFA was also able to obscure the source of some comments by creating unique comment texts. As described above, a BFA subcontractor used software and a template with Mad Libs–style blanks to create distinct comment text for 1 million comments. An observer reviewing these comments would be given the false impression that the comments were submitted independently of each other, and reflected grassroots support for the repeal of the FCC's net neutrality rules.

D. The Broadband Industry Sent Over Half a Million Letters to Congress

At the same time that BFA's campaign to influence the FCC's rulemaking proceeding was underway, BFA engaged in a related effort to influence legislators. Just like the attempts to use comments to affect agency rulemaking, these efforts yielded the submission of millions of fraudulent letters to lawmakers.

At BFA's direction, in May 2017, BFA's lobbying firm engaged a vendor to email letters to Republican members of Congress on behalf of their constituents. These emailed letters were reformatted versions of the same comments collected by Fluent and sent to the FCC. As in the versions sent to the FCC, none of the messages were actually authorized by their signatories.

The fake messages were sent to more than 200 Republican senators and representatives. Each received hundreds or thousands of these messages. Senator Rob Portman — who chaired the Senate Permanent Subcommittee on Investigations in 2019 when it issued a report on abuses of the federal notice-and-comment rulemaking process — was sent more than 14,000 fake messages. As described below, the campaign was cut short after several people reported that they had never authorized the messages that had been sent to members of Congress on their behalf. By that point, between 300,000 and 500,000 fake messages had already been submitted.

While that campaign was still in progress, BFA engaged Fluent for two ***additional*** campaigns, focused on generating letters with messages tailored to members of Congress. One campaign targeted Democrats, the other targeted Republicans.[35] In both campaigns, Fluent was directed to run a campaign solicitation on its co-registration sites to obtain individuals' consent for the submission of a message to their members of Congress. As in the comment campaigns, Fluent fabricated all of the records of consent it claimed to have obtained. As a result, the vendor sent nearly 360,000 additional fraudulent letters to members of Congress.

The OAG has seen no indication that any member of Congress was ever informed that the hundreds or thousands of letters he or she received in these campaigns were fraudulent.

E. The Broadband Industry's Campaign Organizers Ignored Red Flags of Fraud and Impersonation

Although the OAG does not have evidence that BFA or its lobbying firm had direct knowledge of the fraud at the inception of the campaign, several significant red flags appeared shortly after the campaign started, and continued for months yet still remained unheeded. Emails obtained by the OAG reveal that all of these indications of fraud were seen and discussed by BFA's lobbying firm. While BFA was aware of some of the same red flags its lobbying firm saw, it is unclear if the lobbying firm brought other red flags to BFA's attention. As explained above, one of the vendors that BFA's lobbying firm had hired lied when confronted with some of these complaints of fraud. In the end, despite the presence of the red flags, BFA and its lobbying firm continued to use the same campaign vendors to generate comments.

Shortly after BFA began to submit comments to the FCC, in early May 2017, reports began to appear in the press of individuals who stated on the record that comments using their names and addresses had been submitted without their consent.[36] BFA and its lobbying firm were aware of these accounts, discussing and linking to them in emails obtained by the OAG.[37] By mid-May, one of the campaign sponsors had relayed to BFA's lobbying firm additional accounts of impersonation from the individuals who claimed their names and addresses had been used in comments without their consent.[38]

In June 2017, the vendor that was retained to email letters to members of Congress also began receiving reports of constituents who claimed their names and addresses had been misused in messages that they had never seen or authorized. For example, in messages forwarded to BFA's lobbying firm, one outraged individual wrote, "How did u get my email address and why are u sending shit to a congressman through my email. I suggest you contact me back on this matter and explain yourself . . . ." Another complaining individual explained that she had "never even heard of Net Neutrality" and demanded to know who was behind the use of her identity without her knowledge.

The email vendor became alarmed and informed BFA's lobbying firm on June 29, 2017 that "We have serious concerns about the validity of the people taking action on these campaigns." By mid-July, the vendor stopped submitting comments to Congress. When the lobbying firm raised these issues with Fluent, who had supplied the comments that were used in the letters, Fluent repeatedly and deliberately misled the lobbying firm to conceal its fraud. The email vendor, however, investigated further, contacting several of the individuals who had complained to their members of Congress. These individuals uniformly stated that they had never visited Fluent's websites or agreed to participate in the net neutrality campaigns. Several days after it suspended the campaign, the email vendor terminated its engagement with BFA's lobbying firm and refused to send any additional comments Fluent had provided.

Despite these reports and concerns, BFA's lobbying firm continued to allow Fluent to run the net neutrality comment campaign and continued to submit comments to the FCC based on the consent Fluent claimed to have obtained.[39]

2. More than 9.3 Million Additional Fake Comments Using Fictitious Identities Were Submitted to the FCC with Automated Software

In addition to the more than 8.5 million fake comments submitted to the FCC through BFA's campaign opposing net neutrality, more than 9.3 million fake comments were submitted to the FCC that expressed support for net neutrality. These comments differed from the comments submitted in the BFA campaign in two critical respects. First, unlike the comments submitted through the BFA campaign, these pro-neutrality comments did not use the names or addresses of real people, and instead used fictitious identities. Second, these fake comments were submitted to the FCC one-by-one, using software capable of rapidly submitting comments without user interaction.

A. A 19-Year-Old College Student Submitted Over 7.7 Million Fake Comments In Support of Net Neutrality Using Fictitious Identities

The OAG found that a 19-year-old college student in California pursuing a degree in computer science submitted more than 7.7 million comments expressing support for net neutrality. All of the comments were fabricated. However, unlike the comments submitted through the BFA campaign, none of the 7.7 million comments used the names or addresses of real people. Instead, the identities of the purported commenters were generated by randomly combining first names, last names, street numbers, street names, and cities, likely using a website called Fake Name Generator (fakenamegenerator.com).

In addition, all of the comments used "disposable" email addresses. Disposable email addresses allow anonymous access to an email account, typically for a short period of time. All of the 7.7 million comments used email addresses that were issued by a single disposable email address service — Wegwerf-eMail-Adresse — which offered disposable email addresses from ten seemingly unrelated email domains, including @cuvox.de, @dayrep.com, and @superrito.com.[40] The Fake Name Generator website could be configured to automatically generate a disposable email address from Wegwerf-eMail-Adresse that matched the first and last name of the fake identity it generated.

The student submitted each of the 7.7 million comments to the FCC website, one-by-one, using software capable of rapidly submitting comments without user interaction. The government systems had few safeguards in place to detect or prevent millions of submissions from a single individual.

B. An Unknown Party Submitted More Than 1.6 Million Comments Using Fictitious Identities

In addition to the comments described above, the OAG identified a distinct group of more than 1.6 million fake comments that expressed support for net neutrality. Like the comments submitted by the 19-year old college student, these comments used fictitious identities generated by randomly combining name and address information. These comments, however, used different email address domains — pornhub.com, hurra.de, yahoo.de, yahoo.fr, and mail.ru — and mailing addresses in Germany, France, Russia, and the United States. The comments were also submitted, one-by-one, using software capable of operating without user interaction. The OAG has not identified the source of these comments or determined whether they were submitted by a foreign or domestic actor.

3. Lead Generators Corrupted Over 100 Other Advocacy Campaigns with 4.6 Million More Fraudulent Comments and Messages That Impersonated Real People

In the course of its investigation, the OAG found that three of the lead generation firms involved in the net neutrality comment campaigns had also worked on other, unrelated campaigns to influence regulatory agencies, lawmakers, and public officials. The lead generation firms played the same role in those campaigns: to obtain individuals' consent to submit comments, letters, and petitions to the government on their behalf.

Between 2015 and 2018, these three lead generators ran 119 advocacy campaigns, comprising at least five campaigns to generate public comments for agency rulemaking proceedings and 114 campaigns to submit letters and petitions to legislators and other government officials. Across these campaigns, the three lead generation firms provided their clients with the names and information of approximately 4.6 million individuals, all of whom the firms claimed had approved the submission of a comment, letter, or other message to the government on their behalf. The OAG found, however, that in nearly all of these advocacy campaigns the lead generation firms had engaged in fraud, just as they had done in the net neutrality campaigns.

A. Fluent

Fluent, the lead generation firm described above that was responsible for the largest number of fake comments in BFA's net neutrality campaign, began marketing its services for political advocacy campaigns in 2016. From that time until shortly after it received the OAG's subpoena in 2018, Fluent ran 82 political advocacy campaigns in addition to the net neutrality campaigns. In each of these campaigns, Fluent was engaged to run solicitations seeking individuals' consent to submit advocacy messages to the government on their behalf. The campaigns involved a wide array of issues, including criminal justice reform, data privacy, energy and drilling, gambling, health care, taxes, and tobacco. Several of these campaigns were large: eight involved more than 100,000 individuals, and another 33 involved more than 10,000 individuals. In most of these campaigns, the advocacy messages were sent as letters or petitions to members of Congress, state legislators, or other government officials.

The OAG found that Fluent fabricated every single record of consent in each of these 82 campaigns. In most campaigns, the company never even presented the political advocacy solicitation to visitors on its co-registration websites. Instead, as in the net neutrality comment campaign, the company simply copied the names and contact information that visitors supplied to its co-registration websites to win prizes, and falsely represented to its clients that these individuals had agreed to participate in the campaign. Across all of the campaigns, Fluent faked consent for the submission of more than 3.6 million advocacy messages.

The results in one of these campaigns illustrates the scale and impact of Fluent's fraud. In 2016, Fluent helped generate comments for an FCC rulemaking proceeding concerning data privacy.[41] The fake comments that were ultimately submitted to the FCC based on Fluent's work swamped all others: out of the 276,000 total comments submitted to the FCC prior to the agency's adoption of data privacy rules in October 2016, nearly 250,000 — or over 90% — were generated from the fake records of consent Fluent had provided its client.

B. Digital Advertising Firm

The digital advertising firm described above, which falsely claimed it had used online advertisements to obtain consent from 1.5 million individuals for the submission of comments to the FCC, worked on at least five other advocacy campaigns between 2016 and 2018. The company was engaged in these campaigns for the same purpose: to obtain individuals' consent for the submission of advocacy messages to the government using online advertisements. In four of the campaigns, the advocacy messages were submitted as comments to federal agencies in rulemaking proceedings, including an FCC proceeding unrelated to net neutrality and proceedings of the Environmental Protection Agency and the Bureau of Energy Management at the U.S. Department of the Interior. In the fifth campaign, the messages were sent to state legislators.

The OAG has determined that in at least three of these campaigns, the advertising firm fabricated all or nearly all of the records of consent.[42] The names and addresses in these records, which the firm claimed had been collected from individuals who had provided their consent, had in fact merely been copied. As in the net neutrality campaign, some of the records were created by copying personal information that had been stolen in a data breach and released online. The bulk of the records, however, were created using information the advertising company's own client had supplied. This information — lists of individuals who were expected to be supportive of the campaigns' messaging — were intended to be used to target the online advertisements. Instead, the advertising company simply repackaged the information its client had provided and represented that those individuals had responded to the campaign advertisements. Across the three campaigns, the digital advertising company fabricated consent for the submission of more than 830,000 advocacy messages.

C. React2Media

React2Media is one of the five co-registration firms that fabricated consent for approximately 329,000 individuals in BFA's Comment Campaign 2, concerning net neutrality, as described above. The OAG found that React2Media was also engaged in at least 34 other advocacy campaigns between 2015 and 2018. The company's role in these campaigns was also to solicit and obtain individuals' consent to submit advocacy messages to the government on their behalf. Unlike the net neutrality campaign, these campaigns involved only letters or petitions to legislators and government officials, not comments to a regulatory agency. The campaigns concerned a variety of issues, including environmental protection regulations at the federal and state levels, United States foreign policy, and the legalization of online gambling in New York.

The OAG found that, as in the net neutrality comment campaign, the co-registration firm fabricated all, or nearly all, of the records of consent for these campaigns using personal information copied from older co-registration data. And as in the net neutrality campaign, the firm generated fake timestamps for the records that purported to reflect when individuals had viewed the campaign and provided consent. In all, across the 34 campaigns the co-registration firm supplied records of consent for the submission of more than 160,000 advocacy messages, all or nearly of which were fabricated.

Recommendations

As this report makes clear, deception and fraud have infected public policymaking by agencies and legislatures, drowning out citizens' voices with manufactured and fraudulent public comments, letters, and petitions (collectively referred to as "comments and messages" in this Recommendations section of the report). Reform is badly needed.

In Part 1 below, we identify steps advocacy groups should take to ensure they have obtained valid consent from an individual before submitting a comment or message to the government on their behalf. In Part 2, we identify steps agencies and legislatures that manage electronic systems for receiving comments and messages should take to hold the advocacy groups and their vendors more accountable for the comments they submit on behalf of individuals. In Part 3, we propose new laws aimed at those engaging in or facilitating fraud, to better prevent misconduct and hold fraudsters to account for their deception. Finally, in Part 4, we recommend the adoption of various technical safeguards to protect against unauthorized bulk submissions using automation.[43]

The reforms in Parts 1, 2, 3, and 4 are all necessary parts of the solution.

1. Advocacy Groups Must Ensure Valid Consent

The following recommendations mirror the comprehensive reforms that the OAG imposed through its settlements with lead generation companies. Such measures should guide advocacy groups in developing advocacy campaign solicitations and in their use of vendors to assist them with campaigns.

A. Obtain Express, Informed Consent

In its investigation, the OAG identified several campaigns that solicited individuals' participation without adequate disclosures. Some of these solicitations failed to clearly disclose that a comment or message would be sent on behalf of the individual, some failed to provide the content of the comment or message that would be sent, and some failed to disclose the intended government recipient. The problem was compounded because of where solicitations appeared: on co-registration websites, where consumers may be focused on obtaining prizes and where they are not expecting to see solicitations for policy advocacy.

Advocacy groups should only submit a comment or message on behalf of an individual if they, and any vendors they use, have obtained that individual's express, informed consent. To obtain express, informed consent, a solicitation would, at a minimum, have to clearly and conspicuously (a) disclose to the individual that a comment or message would be sent to the government on their behalf and (b) specify the individual's personal information that would be included. The solicitation would also have to make the full text of the comment or message readily available, either adjacent to the other disclosures or through a clearly labeled and conspicuous hyperlink.

B. Properly Oversee Vendors

In the broadband industry's net neutrality campaign, BFA had little understanding of whether and how the vendors it was funding actually obtained consent from individuals to submit comments on their behalf. This was likely in part because it was separated from most lead generators by three or four layers of intermediaries and in part because it had little incentive to closely scrutinize the results.

Advocacy groups should closely supervise their vendors to confirm that they have obtained individuals' express, informed consent to submit a comment or message on the individuals' behalf. In light of the pervasive fraud the OAG has uncovered, this duty must extend beyond passively accepting assurances from their service providers. Instead, before a campaign starts, advocacy groups should proactively identify who will solicit consent — both the vendors and the subcontractors those vendors hire — and how. In addition, during the campaign, the advocacy group should take reasonable steps to verify that consent was obtained as expected. This would include, at a minimum, requiring that each vendor (and any subcontractors) provide the address of the webpage or location through which consent was solicited, a screenshot or image of the solicitation, the date and time that the individual provided consent, and the IP address the individual used at the time they provided consent. Finally, advocacy groups should thoroughly investigate any complaints or reports of fraudulent comments and messages and not merely rely on assurances from the vendors who have incentives to explain away lapses.

2. Agencies and Legislatures Must Make Intermediaries Accountable

The abuses detailed in this report largely stem from intentional fraud by intermediaries standing between citizens and the government. To curb these abuses, intermediaries must be made accountable. Towards that end, the OAG has outlined below requirements that government agencies and officials accepting comments or messages should impose on intermediaries. The requirements should be imposed on any person or entity that submits comments or messages on behalf of others, or funds, organizes, or operates a campaign to submit such comments or messages, regardless of whether it is a non-profit advocacy group or a for-profit company hired to assist with a campaign. Lawmakers should, to the extent necessary, grant agencies authority to adopt these reforms, mandate their adoption to ensure that they are implemented uniformly and consistently, and provide agencies with the resources to do so.

A. Mandate Disclosure

A central challenge in investigating abuse in a regulatory proceeding is tracing fraudulent comments back to their sources. To facilitate accountability, intermediaries should be required to disclose, with each comment or message submitted, the intermediary's own identity and the identities of any parties that assisted in the generation or submission of the comments and messages. Disclosure could be effectuated either within the text of a comment or message (e.g., "This comment was solicited and submitted by Company A, on behalf of Non-Profit X.") or separately in viewable metadata attached to the comments and messages (e.g., requiring registration for mass submissions).

This disclosure should also be available to the public as part of any public comment process. The information would inform public debate by revealing the involvement of interested parties who would otherwise remain hidden, in some cases deliberately so. It would also enable members of the public and the press to help identify abuses. Additionally, it would help rebuild public trust in a system that has been abused.

GSA, the federal agency that operates Regulations.gov — the comment collection website used by many federal agencies (though not the FCC, SEC, and others) — has already taken some steps to improve disclosures in certain rulemaking proceedings. Every entity seeking authorization to use the Regulations.gov application programming interface (API) to submit comments must first identify itself. GSA then uses a commercial provider of identity validation services to verify the entity's identity.[44] This system provides a good starting point, but more is needed. All agencies — whether they use Regulations.gov or not — should require that advocacy groups that sponsor or run campaigns, and not just their vendors, be identified, and should ensure that any identifying information that is submitted be made available to the public.

Similarly, where legislators and other government officials (as opposed to agencies) use electronic systems to accept advocacy messages, as Congress does through its email system, should require intermediaries to disclose themselves.

B. Hold Intermediaries to Account

Advocacy groups' effectiveness and relevance is typically measured by their ability to engage large numbers of people and drive them to take action. These groups, and the vendors they use, have little incentive to root out fraud in their own campaigns. This report documents the result of such lack of accountability: more than 13.1 million fake comments and messages generated by advocacy groups across the net neutrality proceeding and more than 100 other advocacy campaigns.

To stamp out rampant fraud, the incentives must change. Advocacy groups and the vendors that they use should be held accountable for the fake comments and messages they submit to government. This would place responsibility on the parties best positioned to actually detect and prevent fraud.

To hold intermediaries accountable, agencies should impose consequences for fake submissions. Those consequences might vary based on several factors, such as the number of fake submissions attributable to the intermediary, whether those submissions were inadvertent or intentional, and what measures the intermediary had put in place in advance to prevent fake submissions. Any intermediary that abuses the system should have their submission privileges suspended.

3. Lawmakers Must Strengthen Laws to Better Deter Deception and Impersonation

The bulk submission of unauthorized comments and messages can have wide-ranging and significant consequences: it can misdirect regulation and legislation, impede agencies' operation, undermine public confidence in the regulatory process, and drown out or dilute the voices of parties who have a genuine interest in the policy issue.

Under certain circumstances, the submission of unauthorized comments or messages violates existing federal and state laws.[45] But these statutes of general applicability are not sufficiently tailored to address the issues that arise in the context of unauthorized comments and messages. Congress and state legislatures should therefore take the following actions:

A. Prohibit deceptive and unauthorized comments

Congress and state governments should prohibit knowingly submitting, or causing to be submitted, two or more comments or messages to the government (a) that are intended to deceive or (b) on behalf of someone else without first using reasonable measures to verify the comments or messages were authorized through express, informed consent. A federal law would effectively require advocacy groups to take appropriate steps to confirm that individuals had provided valid consent for the submission of comments and messages on their behalf. The law would also prohibit most types of fake comments and messages, including submissions using fictitious identities that are intended to deceive.[46]

The law should establish meaningful penalties for violations, including substantial civil fines that make fraud costly, not merely a cost of doing business. In addition, state attorneys general should be expressly authorized to enforce these statutes in situations where their state's residents' information has been misused.

B. Strengthen impersonation laws

Under federal law, it is illegal in some circumstances to lie to the government, to copy another person's identity, and to interfere with government processes. In New York, it is a misdemeanor to impersonate another by website or electronic means with intent to obtain a benefit. These criminal statutes were not designed to deter the misuse of hundreds of thousands of individuals' identities. Congress and state governments — including New York's legislature — should amend impersonation laws to provide for substantial penalties when many individuals are impersonated before a government agency or official.

4. Agencies and Legislatures Must Implement Technical Safeguards Against Automated Submissions

When the FCC opened the net neutrality rulemaking proceeding in mid-2017, there were few, if any, measures in place to prevent people from using automated software to submit comments through its website. As a result, a 19-year-old college student using software was able to single-handedly submit more than 7.7 million fabricated comments in the net neutrality regulatory proceeding.

Since that time, federal agencies have begun to take steps to address the issue. GSA, the federal agency that operates the Regulations.gov website, recently announced[47] that it had implemented a security feature, known as CAPTCHA, to block automated submissions of comments.[48] The FCC has also stated that it is investigating various options for its own comment submission system, including CAPTCHA.[49]

Implementing CAPTCHA tests would be a good first step to combatting automated software, and agencies should do so immediately. But CAPTCHA tests alone will be insufficient to defeat determined attackers. Fortunately, there are a variety of existing technical measures that can monitor for and mitigate automated traffic and that could be implemented without encumbering individuals' participation in regulatory proceedings. These range from simple techniques, such as rate limiting, to sophisticated third-party bot detection services. Agencies should investigate and implement appropriate strategies.

Where budget shortfalls preclude government funding for new technologies, the OAG calls on civic-minded private sector actors to partner with government to implement these technologies.

Endnotes

1 *See* Brian Fung, "This poll gave Americans a detailed case for and against the FCC's net neutrality plan. The reaction among Republicans was striking.," The Washington Post (Dec. 12, 2017), *available at* washingtonpost.com/news/the-switch/wp/2017/12/12/this-poll-gave-americans-a-detailed-case-for-and-against-the-fccs-net-neutrality-plan-the-reaction-among-republicans-was-striking.

2 *See, e.g.,* Merriam-Webster.com (defining "astroturfing" as "organized activity that is intended to create a false impression of a widespread, spontaneously arising, grassroots movement in support of or in opposition to something (such as a political policy) but that is in reality initiated and controlled by a concealed group or organization (such as a corporation)," *available at* merriam-webster.com/dictionary/astroturfing.

3 Such risks are not merely theoretical, as OAG detailed in a comment to the FCC during the net neutrality proceeding: "[The OAG] investigations have uncovered documentary evidence revealing — for the first time — that from at least 2013 to 2015, major [broadband providers] made the *deliberate business decision* to let their networks' interconnection points become congested with internet traffic and used that congestion as leverage to extract payments from backbone providers and edge providers [such as Netflix], despite knowing that this practice lowered the quality of their customers' internet service. This practice was . . . used for years by at least two of the country's biggest [broadband] providers who operate in New York and in many other states." *See* People of the State of New York Comments on the May 23, 2017 Notice of Proposed Rulemaking in Restoring Internet Freedom, WC Docket No. 17-108 (emphasis in original) (footnotes omitted), *available at* fcc.gov/ecfs/filing/10717583023587.

4 See endnote 1 above.

5 These requirements are laid out in the Administrative Procedure Act, 5 U.S.C. § 551 *et seq.,* and other federal statutes.

6 *See, e.g.,* Chris Sinchok, "An Analysis of the Anti-Title II bots," Medium.com (May 14, 2017), *available at* medium.com/@csinchok/an-analysis-of-the-anti-title-ii-bots-463f184829bc.

7 *See, e.g.,* Zack Whittaker, "Anti-net neutrality spammers are flooding FCC's pages with fake comments," ZDNet.com (May 10, 2017), *available at* zdnet.com/article/a-bot-is-flooding-the-fccs-website-with-fake-anti-net-neutrality-comments; Emily Allen, "7,000-plus Coloradans' names, addresses used to post fake comments about government decision," FOX31 Denver KDVR-TV (May 14, 2017), *available at* kdvr.com/news/7000-coloradans-names-addresses-used-to-post-fake-comments-about-government-decision.

8 *Id.*; Daniel Oberhaus, "Dead People Are Posting Anti-Net Neutrality Comments to the FCC Website," Motherboard (May 25, 2017), *available at* motherboard.vice.com/en_us/article/dead-people-are-posting-anti-net-neutrality-comments-to-the-fcc-website.

9 See discussion in OAG's Findings, § 1(D)..

10 Campaign proposal document, attached to January 2017 email from BFA's lobbying firm to BFA.

11 *Id.*

12 Campaign planning document and budget, attached to March 2017 email between BFA executive committee members and BFA's lobbying firm.

13 Campaign planning documents, budgets, invoices, and emails, dated January 2017 through January 2018, between BFA executive committee members and BFA's lobbying firm.

14 *Id.*

15 Campaign planning document from April 2017.

16 Campaign planning document, attached to March 2017 email between BFA executive committee members and BFA's lobbying firm.

17 May 2017 email to BFA executive committee members.

18 May 2017 emails from BFA's lobbying firm to BFA executive committee members.

19 May 2017 emails between BFA's lobbying firm and BFA executive committee members discussing comment volumes and lobbying firm recommendations for pace and volume of comment submissions; January 2018 BFA budget documents showing total spending and comment volumes that BFA ultimately approved for all of 2017.

20 August 2017 emails between BFA's lobbying firm and BFA executive committee members.

21 *Id.*

22 Press Release, "FCC Comments on Net Neutrality & Title II: A Comprehensive Analysis," Broadband for America (Aug. 30, 2017), *available at* broadbandforamerica.com/2017/08/30/fcc-comments-net-neutrality-title-ii-comprehensive-analysis.

23 See discussion in OAG's Findings, § 1(D).

24 January 2018 BFA budget documents showing spending on campaign, including for comments.

25 *Id.* The funds were also spent on public relations, social media, and related activities to promote public comments opposing net neutrality. *Id.*

26 January 2018 BFA budget documents showing contributions by BFA member broadband companies and trade groups.

27 *Id.*

28 Reporting on astroturfing has found that such obfuscation is a primary goal and benefit. For example, in 2014, a leaked recording revealed how one individual who sold astroturfing services to corporate clients told a gathering of oil industry executives, "People always ask me one question all the time: 'How do I know that I won't be found out as a supporter of what you're doing?' . . . We run all of this stuff through nonprofit organizations that are insulated from having to disclose donors. There is total anonymity. People don't know who supports us." Eric Lipton, "Hard-Nosed Advice from Veteran Lobbyist: 'Win Ugly or Lose Pretty,'" N.Y. Times (Oct. 30, 2014), *available at* nytimes.com/2014/10/31/us/politics/pr-executives-western-energy-alliance-speech-taped.html.

29 Like Fluent, the companies further down the chain all operated co-registration websites that offered incentives to individuals who agreed to provide their personal information to marketers.

30 For clarity, Figure 7 omits co-registration companies responsible for 30,000 or fewer records of consent.

31 The remainder of the comments — approximately 80,000 — originated from co-registration companies that had only provided consent for between a few hundred and 30,000 comments. The OAG has not determined the provenance of these comments.

32 The records were taken from a data breach suffered by Modern Business Solutions, a company that provided data management services.

33 The OAG has not yet determined the source for the name and address information used in approximately 6,000 of the more than 1.5 million comments.

34 May 2017 emails between BFA's lobbying firm and vendors.

35 The message targeting Democrats called on the recipient to "work with your colleagues on a bipartisan law" that would replace the existing robust net neutrality regulations with legislation that had weaker protections the broadband industry favored. The message targeting Republicans abandoned the language of bipartisanship and urged the recipient to enact industry-friendly legislation to "shut the door forever on overregulation of the internet."

36 *See, e.g.,* Zack Whittaker, "Anti-net neutrality spammers are flooding FCC's pages with fake comments," ZDNet.com (May 10, 2017), *available at* zdnet.com/article/a-bot-is-flooding-the-fccs-website-with-fake-anti-net-neutrality-comments/; Daniel Oberhaus, "Dead People Are Posting Anti-Net Neutrality Comments to the FCC Website," Motherboard (May 25, 2017), *available at* motherboard.vice.com/en_us/article/dead-people-are-posting-anti-net-neutrality-comments-to-the-fcc-website.

37 May 2017 emails between BFA's lobbying firm and BFA's executive committee.

38 May 2017 emails between BFA's lobbying firm and one of the non-profit campaign sponsors and two for-profit lead generators the lobbying firm had engaged on BFA's behalf.

39 See discussion in OAG's Findings, § 1(A), concerning findings from the OAG's investigation of the for-profit firm BFA continued to use through mid-August 2017 to carry out its astroturfing campaigns.

40 The full list of Internet domains are: @armyspy.com, @cuvox.de, @dayrep.com, @einrot.com, @fleckens.hu, @gustr.com, @jourrapide.com, @rhyta.com, @superrito.com, and @teleworm.us.

41 The proceeding was entitled "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," WC Docket No. 16-106.

42 The OAG has not yet determined whether the records of consent in the remaining two campaigns, comprising nearly 118,000 records, were fabricated.

43 The recommendations would not foreclose anonymous comments and messages, which some agencies and officials find valuable to engage the public while preserving privacy. Although it can be more challenging to verify that anonymous comments and messages reflect genuine views of actual people, the steps we outline below provide robust protection against fraud while preserving the public's privacy interests.

44 gsa.gov/policy-regulations/regulations/managing-the-federal-rulemaking-process.

45 *See, e.g.,* 18 U.S.C. § 1001, which prohibits making false statements; 18 U.S.C. § 371, which has been held to prohibit conspiring to impair, obstruct, or defeat the lawful function federal government; N.Y. Penal Law § 190.25, which prohibits certain types of impersonation.

46 A comment or message that is signed "anonymous" would not reflect an intent to deceive and should not be penalized, for reasons described above in endnote 43.

47 gsa.gov/policy-regulations/regulations/managing-the-federal-rulemaking-process.

48 "CAPTCHA" is an acronym that stands for "Completely Automated Public Turing test to tell Computers and Humans Apart." CAPTCHA tests typically require that a user prove she is human by completing a task that would be difficult for software, such as identifying a photograph of a bicycle or crosswalk.

49 Report, "Abuses of the Federal Notice-and-Comment Rulemaking Process," U.S. Sen. Permanent Subcommittee on Investigations, p. 24, *available at* hsgac.senate.gov/imo/media/doc/2019-10-24%20PSI%20Staff%20Report%20-%20Abuses%20of%20the%20Federal%20Notice-and-Comment%20Rulemaking%20Process.pdf.