



ELECTRONIC FRONTIER FOUNDATION

Protecting Rights and Promoting Freedom on the Electronic Frontier

February 11, 2018

The Honorable Andrew Zwicker
Chair
Assembly Committee on Science,
Innovation, and Technology
Committee Room 12, 4th Floor
State House Annex
Trenton, NJ 08625

The Honorable James Kennedy
Vice-Chair
Assembly Committee on Science,
Innovation, and Technology
Committee Room 12, 4th Floor
State House Annex
Trenton, NJ 08625

Re: Federal Communications Commission's December 14, 2017 decision to end oversight over Internet Service Provider industry and its impact on privacy and network neutrality

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 41,000 dues-paying members and well over 1 million followers on social networks, we focus on promoting policies that benefit both creators and users of technology. We provide the following analysis for the New Jersey legislature in its effort to respond to the Federal Communications Commission's (FCC) decision to abandon its responsibility to protect user privacy and network neutrality.

GENERAL RECOMMENDATIONS

Given The FCC's Decision to Abdicate its Traditional Role in Protecting User Privacy and Network Neutrality, New Jersey Should Endeavor to Fill the Gap to the Extent Permitted by Law.

The FCC made it clear that it will no longer seek to protect user privacy or network neutrality.¹ However, that unfortunate decision creates an opportunity for states to take on greater oversight role themselves. The FCC has reclassified broadband providers as subject to regulation under Title I of the Communications Act of 1934, rather than Title II. This matters because Title I carriers are subject to relatively no federal statutory obligations. Therefore, state laws regulating their conduct are unlikely to come into conflict with federal law. In addition, Congress has never expressly preempted the states from regulating companies that communicate by wire or radio in their entirety. In fact, Congress explicitly empowered states over the “charges, classifications, practices, services, facilities, or regulations for or in connection with *intrastate* communication service by wire or radio of any carrier (emphasis added).”²

¹ FEDERAL COMMUNICATIONS COMMISSION, *Restoring Internet Freedom Declaratory Ruling, Reporting and Order, and Order* (Dec. 14, 2017), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-166A1.pdf.

² 47 U.S.C. § 152(b).



As a result of the current legal landscape facing consumers, EFF recommends that the legislature take steps to respond to the federal retreat on oversight of the broadband industry.

First, it should be understood that the FCC did more than repeal network neutrality but also eliminated the last vestiges of consumer privacy for cable or telephone companies. Late in 2016, the FCC issued strong rules requiring ISPs to secure the consent of their users before being allowed to monetize their personal data. In 2017, Congress repealed those rules via the Congressional Review Act.³ In effect, the repeal eliminated the updated privacy rules for broadband providers and prohibited the FCC from reviving identical or “substantially similar” rules in the future. Whatever powers remained at the FCC⁴ to protect user privacy was completely eliminated by the agency’s decision to reclassify broadband as Title I information services. In the absence of federal law and completely abdication of duty by the expert federal agency, only state law remains as the means to restore user privacy in the broadband marketplace. The Assembly legislation, A1527, would effectively restore the privacy rules in state law form.

Second, the legislature should pass a legally enforceable and narrowly targeted state based network neutrality law. To survive judicial scrutiny, any such law should be premised on intrastate regulation. No state law will be able to replace in its entirety what was lost with the repeal of the Open Internet Order in December due to the limitations created by the Commerce clause, but states have a valuable role in promoting a free and open Internet by leveraging state power. Connecting network neutrality obligations to state power over rights of way, taxpayer funded infrastructure, taxpayer provided subsidies, and state contracts would ensure that residents can enjoy a free and open Internet to the fullest extent state law can provide until the federal protections can be restored. Governor Murphy having issued an Executive Order⁵ tying access to state contracts to following network neutrality has already accomplished one of these approaches.

³ Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 47 CFR 64, available at <https://www.federalregister.gov/documents/2016/12/02/2016-28006/protecting-the-privacy-of-customers-of-broadband-and-other-telecommunications-services>.

⁴ It is worth noting that the FCC asserted to Congress that it retained authority to protect user privacy under its Title II common carrier authority even though the FCC Chairman fully intended to abandon its own authority. Amir Nasr, *Pai: FCC Required to Ensure Internet Privacy Even Without Agency Rules*, MORNING CONSULT (March 8, 2017), available at <https://morningconsult.com/2017/03/08/pai-fcc-required-ensure-internet-privacy-even-without-agency-rules>.

⁵ EXECUTIVE ORDER 9, Governor Philip Murphy, available at <http://www.newjersey.gov/infobank/eo/056murphy/pdf/EO-9.pdf>.



BACKGROUND

The FCC’s “Restoring Internet Freedom” Order Effectively Ended Federal Oversight Over the ISP Industry

On December 14, 2017, the FCC issued the Restoring Internet Freedom Order and thereby effectively withdrew federal oversight over the ISP marketplace.⁶ If that Order survives judicial scrutiny, ISPs will be largely left to police themselves in response to market demands – even though the majority of Americans have only one choice for high-speed broadband and, therefore, can’t exert much influence over their providers.⁷ Indeed, the FCC’s decision contradicts the Trump Administration’s own Department of Justice findings regarding the power of ISPs to harm online competition.⁸

Contrary to FCC Chairman Ajit Pai’s claims, this repeal is not a return to any status quo. Prior to 2015 the FCC under both Republican and Democratic leadership attempted to oversee the practices of ISPs to maintain a free and open Internet through different legal theories known as “ancillary jurisdiction,” which was premised on the FCC having wide ranging powers over broadband carriers that were reclassified as Title I information services beginning in 2005. However, after years of battling ISP lawsuits and losing under its Title I authority to regulate, most notably the *Comcast* decision⁹ and the *Verizon* decision,¹⁰ the FCC was forcefully driven to the conclusion in 2015 that its only legal power over the industry was its common carrier (known as Title II) authority.

Abandoning that authority under the Restoring Internet Freedom Order has effectively ended the nondiscrimination obligations of ISPs that served as the legal authority to require network neutrality.¹¹ It has also extinguished the application of communications privacy law¹² and important competition policies smaller ISPs depended on for market entry.¹³ Once the Restoring Internet Freedom Order takes full effect, the ISP industry will for the first time in communications law history, be virtually free from federal consumer protection law, competition policy, and privacy rules.

⁶ Remarks of Chairman Ajit Pai on Restoring Internet Freedom, available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db1128/DOC-347980A1.pdf.

⁷ Jon Brodtkin, *US Broadband: Still no ISP choice for many, especially at higher speeds*, ARSTECHNICA (August 10, 2016), available at <https://arstechnica.com/information-technology/2016/08/us-broadband-still-no-isp-choice-for-many-especially-at-higher-speeds>; See also Jon Brodtkin, *FCC’s claim that one ISP counts as “competition” faces scrutiny in the courts*, ARSTECHNICA (October 10, 2017), available at <https://arstechnica.com/tech-policy/2017/10/fccs-claim-that-one-isp-counts-as-competition-faces-scrutiny-in-court>.

⁸ DEPARTMENT OF JUSTICE, Antitrust complaint (filed November 20, 2017), available at <https://assets.documentcloud.org/documents/4254900/ATT-Antitrust-Complaint.pdf>.

⁹ *Comcast Corp. v. FCC*, 600 F. 3d 642 (D.C. Cir. 2010) (hereinafter Comcast decision).

¹⁰ *Verizon v. FCC*, 740 F. 3d 23 (D.C. Cir. 2014) (hereinafter Verizon decision).

¹¹ 47 U.S.C. § 201; 47 U.S.C. § 202.

¹² 47 U.S.C. § 222.

¹³ 47 U.S.C. § 224; See also the following letter sent by more than 40 ISPs supporting the 2015 Open Internet Order and opposing the FCC decision to repeal, available at https://www.eff.org/files/2017/06/27/isp_letter_to_fcc_on_nn_privacy_title_ii.pdf.



Data Monetization Efforts by ISPs is Unrelated to the Provisioning of Broadband Internet Access Service and is an Intrastate Business Practice Subject to State Law

The Communications Act envisions federal and state partnerships when it is possible to draw a division between intrastate and interstate activities.¹⁴ The Communications Act also allows states to regulate business practices of ISPs so long as the activity being regulated is intrastate. That does not mean that the FCC is empowered to preempt activities that may include some interstate components solely on the premise that interstate commerce also occurs. As the Supreme Court noted in its *Louisiana Public Service Commission* decision,

“[T]he Act would seem to divide the world of domestic telephone service in two hemispheres – one comprised of interstate service, over which the FCC would have plenary authority, and the other made up of intrastate service, over which the states would retain exclusive jurisdiction – in practice, the realities of technology and economics belie such a clean parceling of responsibility.”¹⁵

Consumer protection laws that guard personal privacy and grant a legal right to say no to a business that wishes to monetize personal information are inherently intrastate regulations. Every valuable piece of personally identifiable information is emitted locally, whether geolocation data, the websites you ask your local ISP to transmit to you, or the identity of applications one has installed on their handheld device. The data collection efforts that ISPs will engage in to establish such business arrangements do not require any crossing of state lines to be effective.

Almost every instance of privacy invasion by the ISP industry requires an intrastate activity such as preinstalling software in newly sold phones within a state,¹⁶ injecting undeletable (and formerly illegal) tracking cookies in outbound traffic by their customers,¹⁷ and hijacking the search queries when sent to the local ISP from their customers’ home¹⁸ before they reached the destination point on the Internet. In virtually every instance the infrastructure relied upon for the collection efforts is housed within state lines—from the local server in both wired and wireless instances to the smartphone itself maintaining a log and reporting it to the ISP.

The state should feel free to address these practices to protect the privacy interests of New Jerseyans as that was how Congress intended to strike the balance between state regulations of companies that provide communications by wire or wireless while

¹⁴ 47 U.S.C. § 152(b) (stating that “nothing in this chapter shall be construed to apply or to give the Commission jurisdiction with respect to (1) charges, classifications, *practices*, services, facilities, or regulations for or in connection with *intrastate* communication service by wire or radio of any carrier”)

¹⁵ *Louisiana Public Service Com.n v. F.C.C.*, 465 U.S. 355 (1986).

¹⁶ Jeremy Gillula, *Five Creepy Things Your ISP Could Do if Congress Repeals the FCC’s Privacy Protections*, DEEPLINKS BLOG (MARCH 19, 2017), available at <https://www.eff.org/deeplinks/2017/03/five-creepy-things-your-isp-could-do-if-congress-repeals-fccs-privacy-protections>.

¹⁷ *Id.*

¹⁸ *Id.*



reserving interstate regulation to the FCC.¹⁹ Today, we see many instances of this division of responsibilities such as universal service fund support²⁰, local rights of way regulation of network deployment²¹, and privacy²² for example.

Promoting Individual Broadband User Privacy Promotes Broadband Adoption

Studies and findings made by several federal agencies²³ including the FCC itself show that privacy protections improve broadband adoption as more sensitive information is collected and distributed online. In other words, user power over their personal data correlates with people's willingness to use the Internet for critical economic and social activities. Without rules or laws in place to constrain the desires by the ISP industry to monitor and monetize everything we do online, such concerns may restrain them from making full use of the broadband service, thereby lowering the likelihood of broadband adoption as the public's fear of a loss of privacy grows.

Even if lawmakers were to take the word of industry that they will do everything they can to safeguard the valuable and vast repositories of the personal information of their users, it is important to recognize the role policy still plays in protecting the public. In light of the recent Equifax data breach²⁴ that has compromised the personal information of nearly 1 out of 2 Americans, one very important concession to Congress was made during its investigations. Yahoo's former Chief Executive Officer Marisa Mayer best sums up that concession with the following sentence,

¹⁹ 47 U.S.C. § 152(b).

²⁰ A 2012 study indicates that a vast majority of states provide indirect subsidies towards broadband deployment through telephone service and direct subsidies for broadband service. See NATIONAL REGULATORY RESEARCH INSTITUTE, *Survey of State Universal Service Funds 2012*, available at <https://prodnet.www.neca.org/publicationsdocs/wwpdf/72012nrriusf.pdf>.

²¹ 47 U.S.C. § 224(c) (federal law grants the states the ability to "reverse" preempt the FCC should they choose to directly regulate local infrastructure access.)

²² See Minn. Stat. §§ 325M.01 to .09; See also Nevada Revised Stat. § 205.498

²³ NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities* (May 13, 2016), available at <https://www.ntia.doc.gov/print/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>; See also Federal Trade Commission comments to the FCC, WC Docket No. 16-106 (May 27, 2016), available at https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf (citing how risks to privacy suppress consumer willingness to engage in online transactions and other economic activity); See also FEDERAL COMMUNICATIONS COMMISSION, *2016 Broadband Progress Report*, GN Docket No. 15-191 (January 29, 2016), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-6A1.pdf (noting that "if consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband services, thereby lowering the likelihood of broadband adoption and decreasing consumer demand").

²⁴ The behavior of the data broker industry should be informative as both Equifax and ISPs are subject to the same lack of legal obligations to protect privacy.



“The threat from state-sponsored attacks has changed the playing field so dramatically that today I believe that all companies, even the most well-defended ones, could fall victim to these crimes.”²⁵

EFF has a list of recommendations²⁶ to Congress to address the Equifax breach, but the lesson we must extract from the failure of the data broker industry to safeguard consumer data is that it may not be a question as to whether or not personal information is divulged, but rather when will it happen. More so, when that personal information becomes public through the hands of criminal hackers, what laws were in place to curtail the data monetization efforts of targeted companies best situated to observe and record our most sensitive personal information? A law such as A1527 would reduce the value of personal information if an ISP is legally prohibited from monetizing it with third parties should a user withhold their consent. If the information is not collected due to having lost value, then it will not be disclosed in the aftermath of state sponsored criminal activity.

The ISP Industry Has a Persistent History of Violating Privacy

Nothing in recent history suggests that ISPs stand ready to respect user privacy where they are not legally required to do so. As far back as 2008, Charter tested the idea of recording everything their customers did online into profiles using Deep Packet Inspection technology. The company relented only after bipartisan condemnation.²⁷

In 2011, ISPs engaged in “search hijacking” where your Internet search queries were monitored in order to be rerouted in coordination with a company called Paxfire.²⁸ Other invasive efforts include AT&T inserting ads into data traffic in wifi at airports.²⁹ Even small rural ISPs have engaged in ad injection to advertise on behalf of third parties.³⁰

²⁵ Marisa Mayer, *Prepared Statement before U.S. Senate Committee on Commerce, Science, and Transportation* (Nov. 8, 2017), available at

https://www.commerce.senate.gov/public/_cache/files/55c803e0-2dfe-4027-a698-673742de5e5d/A6ABC76EF5545F8A54933F5F93A0D7B3.11.08.2017---yahoo-testimony.pdf

²⁶ Amul Kalia, *Here’s How Congress Should Respond to the Equifax Breach*, DEEPLINKS BLOG, (Nov. 7, 2017), available at

<https://www.eff.org/deeplinks/2017/11/heres-how-congress-should-respond-equifax-breach>.

²⁷ Press Release, *Markey, Barton Raise Privacy Concerns About Charter Communications* (May 16, 2008), available at <https://www.markey.senate.gov/news/press-releases/may-16-2008-markey-barton-raise-privacy-concerns-about-charter-comm>.

²⁸ Peter Eckersley, *Widespread Hijacking of Search Traffic in the United States*, DEEPLINKS BLOG (August 4, 2011), available at <https://www.eff.org/deeplinks/2011/07/widespread-search-hijacking-in-the-us>.

²⁹ Jonathan Mayer, *AT&T Hotspots: Now with Advertising Injection*, WEB POLICY BLOG (August 25, 2015), available at <http://webpolicy.org/2015/08/25/att-hotspots-now-with-advertising-injection>.

³⁰ Phillip Dampier, *ISP Crams Its Own Ads All Over Your Capped Internet Connection; Banners Block Your View*, STOP THE CAP! (April 3, 2013), available at <http://stopthecap.com/2013/04/03/isp-crams-its-own-ads-all-over-your-capped-internet-connection-banners-block-your-view>.



Carriers also manipulated the software in the smartphones they sell. For example, AT&T, Sprint, and T-Mobile preinstalled “Carrier IQ” on their phones, which gave them the capability to track everything users did with those phones, from the websites they visited to the applications they used.³¹ The carriers abandoned the practice only after a class-action lawsuit.³²

Perhaps the most egregious example, in 2014 Verizon tagged every one of its mobile customers’ HTTP connections with a semi permanent super-cookie, and used those “super-cookies” to enable third parties such as advertisers to target individual customers.³³ Verizon’s “super-cookie” allowed unaffiliated third parties to track an individual, no matter what steps they took to preserve their privacy. AT&T would have followed suit but quickly retreated after Verizon faced an FCC enforcement action.³⁴

Even in the face of the 2015 Title II Open Internet order that would clearly reapply communications privacy law to the industry, they continued to push their conduct as close to the law as possible. In 2015 telecom carriers partnered with SAP’s Consumer Insight 365³⁵ to “ingest” data from cellphones close to 300 times a day every day across 20 to 25 million mobile subscribers (we do not know which mobile telephone companies participate in this practice, as that information is kept a secret). That data is used to inform retailers about customer browsing info, geolocation, and demographic data—information that would be have been clearly protected under the 2016 FCC privacy rules.

The FCC’s Deference to Antitrust Law as Substitute Authority is a Shell Game

Proponents of the repeal pointing towards antitrust law hope that lawmakers have not been paying attention to the erosion of antitrust protections for regulated industries overseen by expert regulatory agencies. The FCC itself regularly asserts that antitrust law can substitute for its authority, while simultaneously acknowledging the regional monopoly challenges consumers face in the high-speed ISP market. Unfortunately our antitrust laws are inadequate for the task of protecting consumers even in the face of dwindling competition.³⁶

³¹ Marcia Hofmann, *Carrier IQ Tries to Censor Research With Baseless Legal Threat*, DEEPLINKS BLOG (November 21, 2011), available at <https://www.eff.org/deeplinks/2011/11/carrieriq-censor-research-baseless-legal-threat>.

³² *In re Carrier IQ, Inc. Consumer Privacy Litigation*, Case No. 12-md-023330 - EMC, available at <http://www.carrieriqsettlement.com> (detailing the terms of the settlement).

³³ Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls*, DEEPLINKS BLOG (November 3, 2014), available at <https://www.eff.org/deeplinks/2014/11/verizon-x-uidh>.

³⁴ FEDERAL COMMUNICATIONS COMMISSION, FCC Settles Verizon “Supercookie” Probe, Requires Consumer Opt-in for Third Parties: Verizon Wireless to Obtain Affirmative Consent from Consumers Before Sending Unique Identifier Headers to Third Parties, available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-338091A1.pdf.

³⁵ Kate Kaye, *The \$24 Billion Data Business That Telecoms Don’t Want to Talk About*, AD AGE (October 26, 2015), available at <http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058/>

³⁶ The seminal Supreme Court cases known as *Trinko* and *Credit Suisse* created a general legal framework where areas of law that have an expert agency with regulatory power over an industry are not benefited by the added layer of antitrust law. As a result, the FCC is expected to exert its oversight over the ISP industry



In 2010, the Federal Trade Commission (FTC) told Congress that if the current status of antitrust law had been in place 40 years ago, the Department of Justice prosecution of AT&T's monopoly would have likely failed.³⁷ Moreover, to the extent that collusive conduct that would run afoul of antitrust laws takes place within the ISP market, the FCC's abandonment of its oversight role will serve as a major obstacle. The Supreme Court, in its *Trinko* and *Credit Suisse* decisions have made it clear that expert regulators should be tasked with resolving industry issues rather than antitrust enforcement actions.

The Residents of New Jersey Cannot Depend on FTC Act Enforcement

The FCC and FTC released a Memorandum of Understanding setting out how the federal government intends to oversee the ISP marketplace.³⁸ The document details the extent the FCC will mandate disclosure by the ISPs of their intended conduct so that the FTC can use its legal power to penalize deceptive assertions. At the heart of the document is a basic premise: as long as the industry simply tells consumers what they intend to do, self-regulation will curtail the worst practices.

This premise cannot withstand scrutiny, for at least two reasons. First, a majority of the public has few if any choices for high-speed broadband, which means they cannot respond to unfair practices, however fully disclosed, by switching providers. Second, it allows ISPs to immunize from legal challenge all of the offending practices listed earlier in this letter so long as they are open about them.

Moreover, the FCC should not have acted in advance of a pending decision regarding FTC authority over telephone companies. Recently, the Ninth Circuit Court of Appeals held that the FTC was legally barred from exerting its authority over the telephone industry.³⁹ The Court is reviewing that decision en banc but, if it is affirmed, the ISPs will have successfully eviscerated even the most basic truth-in-advertising power remaining after the FCC's abdication. In other words, it is possible that neither the FCC nor the FTC will have jurisdiction over telephone companies in many crucial respects in 2018.⁴⁰

in lieu of antitrust law. See *Verizon Communications, Inc. v. Law Offices of Curtis V. Trinko*, 540 U.S. 398 (2004); See also *Credit Suisse Securities v. Billing*, 551 U.S. 264 (2007).

³⁷ Prepared Statement of the Federal Trade Commission, Committee on Judiciary: *Is There Life After Trinko and Credit Suisse? The Role of Antitrust in Regulated Industries* (June 15, 2010), available at https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-courts-and-competition-policy-committee-judiciary-united/100615antitrusttestimony.pdf.

³⁸ FEDERAL COMMUNICATIONS COMMISSION AND FEDERAL TRADE COMMISSION CONSUMER PROTECTION MEMORANDUM OF UNDERSTANDING, available at https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.

³⁹ 15 U.S.C. § 45(a)(2)

⁴⁰ The reason why this decision only applies to telephone companies after broadband is officially declared that it is no longer a common carrier service under the Restoring Internet Freedom Order is because telephone service itself remains a common carrier service allowing companies like AT&T and Verizon to exempt themselves from federal enforcement but not Comcast, Charter, or other cable television companies.



ELECTRONIC FRONTIER FOUNDATION

Protecting Rights and Promoting Freedom on the Electronic Frontier

States Can and Should Act in the Absence of ISP Privacy and Network Neutrality

EFF supports efforts to close the privacy and net neutrality gaps through state legislation and other means of state authority. Americans from across the political spectrum agree that their personal data belongs to them and that they should be able to choose whether and how corporations and the government use it.

A staggering 83% of the public (85% of Republican voters, 82% of Democratic voters, and 78% of independent voters) support requiring ISPs to obtain their permission first before monetizing their personal data.⁴¹ Similarly, an overwhelming majority of the public, Republicans, Democrats, and Independents alike, opposed the FCC's decision to repeal network neutrality.⁴²

In the face of retreat by the federal system, all states should take steps to protect their residents' interests and promote an Internet ecosystem they demand and deserve.

Sincerely,

Ernesto Falcon
Legislative Counsel
Electronic Frontier Foundation

⁴¹ Freedman Consulting, LLC, *New Poll: Americans Overwhelmingly Support Existing Net Neutrality Rules, Affordable Access, and Competition Among ISPs*, available at http://tfreedmanconsulting.com.routing.wpmanagedhost.com/wp-content/uploads/2017/08/Tech-Policy-Poll-Summary-Final_20170710.pdf.

⁴² Brian Fung, *This Poll Gave Americans a Detailed Case For and Against the FCC's Net Neutrality Plan. The Reaction Among Republicans Was Striking*, WASHINGTON POST (Dec. 12, 2017), available at https://www.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/?utm_term=.c5da0e52207b.