Professor Catherine Sandoval
Santa Clara University School of Law
500 El Camino Real
Santa Clara, CA 95053

August 30, 2017

Ms. Marlene Dortch
Federal Communications Commission
455 12th Street S.W.,
Washington D.C. 20554

Re: **Reply Comments, In the Matter of Restoring Internet Freedom, WC Docket No. 17-108, FCC** 17-60

Dear FCC Commissioners and *Internet Freedom* Docket Staff Members;

I. The FCC's Conduct of the *Internet Freedom* Proceeding Constitutes Arbitrary and Capricious Decision-making through its Countenance of Allegedly False Statements Based on Identity Theft and Data Breaches, and Proposals to Allow Paid Prioritization and Remove FCC Jurisdiction Without Sufficient Analysis of the Prior Proceeding Record, Analysis of Consumer Complaints, or Consideration of the Dangers of these Proposals to National Security and American Democracy

Please accept these Reply Comments filed in my individual capacity as a Law Professor at Santa Clara University School of Law urging the FCC, the Federal Bureau of Investigation (FBI), the U.S. Department of Justice (U.S. DOJ), and State Attorneys Generals to investigate the allegations of false federal filings perpetrated through identity theft or data breaches in the FCC's Notice of Proposed Rulemaking (NPRM) *Restoring Internet Freedom*, WC Docket No. 17-108 [hereinafter *Internet Freedom*].[1] Twenty-seven people through a May 25, 2017 letter sent by the organization Fight for the Future Attached as Exhibit A,[2] in addition to technology writer Karl Bode, allege that comments have been filed in this proceeding that use their names and addresses without their authorization to falsely attribute views to them regarding the merits of this proceeding.[3] Another individual, Ryan Clayton, complained to the FCC through the

[1] FCC, *In the Matter of Restoring Internet Freedom*, 82 FR 25568, WC Docket No. 17-108, FCC 17-60, Notice of Proposed Rulemaking (rel. May 23, 2017) (hereinafter *Internet Freedom NPRM*).
[2] Letter to the FCC from people whose names and addresses were used to submit fake comments against net neutrality, May 25, 2017, Fight for the Future, [hereinafter, *False Filing Victim Letter to the FCC*] https://www.fightforthefuture.org/news/2017-05-25-letter-to-the-fcc-from-people-whose-names-and/.
[3] *See*, Karl Bode, *The FCC Insists it Can't Stop Impostors From Lying about My Views on Net Neutrality*, TECHDIRT, July 11, 2017, https://www.techdirt.com/blog/?tag=fake+comments; Letter from Congress Members Frank Pallone, Elijah Cummings, Diana DeGette, Robin Kelly, Mike Doyle, Gerald Connolly to Ajit Pai, Mignon Clyburn, and Michael O'Reily, FCC Commissioners, June 26, 2017, [hereinafter *Congressional letter to FCC re: bot attacks and false filings based on data breaches*] (expressing concern about reports of filings based on identity theft and that more than 150,000 comments were reported to have disappeared from the *Internet Freedom* docket), https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/FCC.Chairman.Commissioners.2017.

comments he posted that "someone previously submitted a comment against "net neutrality" in my name, against my wishes and without my permission."[4] The FCC continues to publicly display most of these allegedly false comments, which include the names and addresses of the identity theft victims.[5] Laila Abdelaziz, Kairos Fellow and Digital Campaigner for Fight for the Future, worked with the identity theft victims to compile information for the May 25 letter to the FCC. In a telephone interview she reported that "the fake comments made in people's name were not necessarily associated always with current addresses, many times, the posted location/ address was a former residence."[6] The FCC has failed to act to take down allegedly false comments, to publicly commit to investigate, or to take the steps to ensure the integrity of the comment process which is integral to notice-and-comment rulemaking. The FCC's failure to address these allegedly false filings based on identity theft reflects arbitrary and capricious decision-making. These false filings also evidence criminal behavior that warrants federal and state investigation.

I am a tenured professor at Santa Clara University School of Law (SCU Law) where I teach and do research on Communications Law, Energy Law, Antitrust Law, and Contracts. I have taught Communications Law at SCU Law since 2004, and taught a Telecommunications,

---

06.26.%20Letter%20to%20FCC%20re%20cybersecurity%20prepardness%20and%20public%20comments.CAT_.OI%5B1%5D.pdf.

[4] *See, e.g.*, Express Comments of Ryan Clayton, July 19, 2017 (requesting that the FCC "remove fraudulently posted comments in my name from the record, which includes any that used my name and stated opposition to "net neutrality."); Express Comments of Ryan Clayton, July 12, 2017 (making the same request for the FCC to remove comments falsely attributed to him); *Cf.* Express Comments of Ryan Clayton, May 11, 2017 (containing an Ohio address in contrast to the Georgia address of the July 12, 2017 and July 19, 2017 Ryan Clayton comments, and listing the same text and filing date as other comments alleged to be falsely filed based on identity theft); Express Comments of John Gentry Williams, June 13, 2017("It's come to my attention that my name submitted 20 times among around 500,000 bogus ECFS comments submitted last month on this brief. I did not make any of those 20 anti-Title II comments and demand that they be deleted."); *cf.* Express Comments of John Williams, May 11, 2017 (containing a different Alabama address than that listed by John Gentry Williams by the same text and filing date as other comments alleged to be falsely filed based on identity theft).

[5] Search of the FCC's Electronic Comments Filing System (ECFS) for FCC Docket No. 17-108, August 4, 2017, conducted by Professor Catherine Sandoval, on file with the author. A screen shot of these filings is not submitted in light of the identity theft allegations by the victims against the comment filer. The ECFS system did not display on August 4 a comment for three names listed on the May 25 letter alleging comments were filed without their authorization, one each in California (Samuel Lewis), Washington (Paulo Llanes), and Michigan (Nicholas Pannuto). The Comments displayed for Angelica Collins from Delaware have different language than other comments alleged in the Fight for the Future letter to be false, and were filed on July 12 and July 13, 2017, as reported by the FCC. ECFS does not display on August 4 comments for another California resident, Richard O. Johnson, listed in the May 25 *False Filing Victim Letter to the FCC*, *supra* note 1, that were before the May 25, 2017 date of the letter to the FCC complaining about the false filings. Some comments bear a different city and state than that listed in the Fight for the Future letter. *See* ECFS, comment posted for Benjamin Currier from a Massachusetts address, not a Colorado address; comment was posted for Cynthia Duby with an address in Monrovia, California, not Desert Hot Springs, CA; comment posted for Daniel Pinkert with an address in Woodbridge, Connecticut, not New York City, NY; comment posted for Greg Baynes with an address in Los Angeles, California, not View Park, CA; comment was posted for Adam Stone with an address in Cropwell, Alabama, not Salt Lake City, Utah; Megan Conschafter, Akron, New York, not Buffalo New York, Surbhi Godsay, Burlington, Vermont, not Nashua, NH; John Ulick, Normal, Illinois, not Champaign, IL, as listed in the Fight for the Future letter.

[6] Telephone Interview with Laila Abdelaziz, Kairos Fellow and Digital Campaigner, Fight for the Future (August 7, 2017).

Broadcast, and Internet Law course at U.C. Berkeley School of Law (formerly Boalt Hall) in 2013. I served a six-year term as a Commissioner of the California Public Utilities Commission from January 2011 to January 1, 2017. The FCC appointed me in November 2011 to the Federal-State Conference on Advanced Services, where I served as State Chair, State Policy Chair, and as a member during my more than five-year tenure. I was a member of the National Association of Regulatory Utility Commissioners (NARUC) Telecommunications Committee from January 2011- January 2017, and served as NARUC Telecommunications Committee Co-Vice-Chair for more than two years. At the FCC, I served as the Director and previously Deputy Director of the FCC's Office of Communications Business Opportunities for five and a half years, and began my FCC service as Special Assistant to the Director of the FCC's Office of International Communications. I submitted comments cited in both the FCC's 2015 and 2010 Open Internet rulemakings.[7] I submit these comments in my individual capacity as a Law Professor, former Commissioner of the California Public Utilities Commission, former FCC Office Director, and citizen. I received no compensation for preparing or filing these comments, apart from my ordinary university salary, and represent no other person or entity through this submission.

These Reply Comments reflect my deep concern about the allegations of lack of integrity in the FCC's *Internet Freedom* rulemaking proceeding. Integrity is at the heart of due process of law and is required to avoid arbitrary and capricious decision-making under the Administrative Procedures Act (APA), 5 USC 551, *et. seq*. Submission of a false statement to a federal agency is a crime under 18 U.S.C. 1001. False statements perpetrated by stealing other people's identities, some of which may be derived from data breaches, raise allegations of state law identity theft crimes, aggravated federal identity theft, and Computer Fraud and Abuse Act violations. The FCC, the FBI, State Attorneys General, and Congress must investigate this proceeding's alleged criminal false filings based on identity theft and data breaches. Authorities must determine the source and motivation for those filings and hold accountable those individuals or organizations – *whether foreign or domestic* – responsible for the alleged identity

[7] *Preserving the Open Internet*, GN Docket No. 09-191, WC Docket No. 07-52, Report and Order, 25 FCC Rcd 17905, n. 112, n. 165, n. 168, n. 170, n. 191 (2010) [hereinafter *2010 Open Internet Order*] (citing Reply Comments of Catherine J.K. Sandoval, Associate Professor of Law, Santa Clara University, Associate Director, Broadband Institute of California, Preserving the Open Internet, Broadband Industry Practices (GN Docket, No. 09-191, WC Docket No. 07-52), at 60, [hereinafter *Professor Sandoval 2010 Preserving the Open Internet Reply Comments]*, https://ecfsapi.fcc.gov/file/7020442044.pdf.). The 2010 Open Internet Order was *aff'd in part, vacated and remanded in part sub nom. Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014); *In re: Protecting and Promoting the Open Internet*, 30 FCC Rcd. 5601, n. 254, 291, 355, 503, 1483 (2015) [hereinafter *2015 Open Internet Order*] (citing Catherine J.K. Sandoval, Commissioner, California Public Utilities Commission, Notice of Ex Parte Communication: Protecting and Promoting the Open Internet, GN Docket No. 14-28; Framework for Broadband Internet Services, GN Docket No. 10-127, received by the FCC October 13, 2014, [hereinafter *Commissioner Sandoval ex parte letter*], https://ecfsapi.fcc.gov/file/60000972786.pdf; Written Statement of Commissioner Catherine J.K. Sandoval, Commissioner, California Public Utilities Commission, Before the Congressional Forum on Net Neutrality, Hosted by Congresswoman Doris O. Matsui, Sept 24, 2014, at 7, 44, 55, 70, 77, 92, 94, 95 [hereinafter *Commissioner Sandoval 2015 Open Internet Ex Parte Comments*]; Catherine J.K. Sandoval, Commissioner, California Public Utilities Commission, State Chair, Federal-State Joint Conference on Advanced Services, November 19, 2014, Section 706, Title II, and the Role of the States; The Open Internet Promotes Critical Infrastructure Safety, Reliability, and Just and Reasonable Rates, at 17, [hereinafter *Commissioner Sandoval Section 706 Chair Submission for 2015 Open Internet Docket*], https://ecfsapi.fcc.gov/file/60001026238.pdf.).

theft, data breaches, and false filings in the FCC's *Internet Freedom* Rulemaking. These issues cannot be addressed merely by giving falsified comments little or no weight in the proceeding, as Chairman Pai has suggested the FCC would do. The FCC's failure to investigate in order to determine which filings are false and their actual source renders if incapable of assessing the weight to give to comments, hundreds of thousands of which are alleged to be false.

Evidence of comments allegedly filed by "bots"[8] based on database breaches or identity theft merits investigation to protect U.S. national interests. More than 444,000 comments filed in this proceeding list the same Russian address. In light of Congressional findings of a Russian influence campaign in 2016 aimed at the United States presidential election,[9] these filings raise grave concerns that a cyber campaign is at work to manipulate U.S. government decision-making. The FCC's rules do not prohibit foreign nationals or entities from commenting on FCC proceedings, and the FCC cooperates with foreign bodies on telecommunications regulations through its International Bureau.[10] Yet, the context of this proceeding frames analysis of comments allegedly submitted from Russia. Those comments must be view in light of the allegations of false filings based on identity theft, the bot swarm that the FCC reported hindered its comment filing system, and the FCC's proposal to allow paid Internet priority without rules or FCC jurisdiction − a proposal which would allow foreign entities or agents to buy U.S. Internet priority. Authorities must determine who is responsible for the apparent ongoing influence campaign to manipulate U.S. government decision-making through false filings, determine whether those responsible are domestic or foreign criminals, and identify their motives.

Identity theft perpetrated through the FCC comment process poses serious threats to participatory democracy through notice-and-comment rulemaking. The FCC must address these threats, stand for the integrity of its rulemaking process as required by the APA, and design a better system to ensure that comments filed by third parties (as FCC rules permit) are filed with the authorization of the named commenter. The FCC should suspend the Internet Freedom rulemaking to investigate these allegations, determine who is responsible, work with authorities to hold accountable those who committed these crimes, and take action if an FCC licensee or their agent is complicit. The FCC should also withdraw the *Internet Freedom NPRM* in light of the proposal's deficiencies, failure to analyze the relevant record, and failure to raise or analyze critical issues such as the NPRM's risks for democracy and national security.

The FCC touts as its "lead proposal"[11] repealing the basis for enforceable rules and reclassifying Internet Service Providers (ISPs) as information service providers. The FCC

---

[8] Webroot, *What are Bots, Botnets, and Zombies* ("Bad bots perform malicious tasks allowing an attacker to take complete control over an affected computer for the criminal to control remotely. Once infected, these machines may also be referred to as 'zombies'"), https://www.webroot.com/us/en/home/resources/tips/pc-security/security-what-are-bots-botnets-and-zombies (last visitied August 6, 2017).

[9] *Countering America's Adversaries Through Sanctions Act*, Pub. L. No. 115-44, 131 Stat 886, Title II (211) (2017) [hereinafter *Countering America's Adversaries Through Sanctions Act*], https://www.congress.gov/bill/115th-congress/house-bill/3364/text?q=%7B%22search%22%3A%5B%22sanctions%22%5D%7D&r=2.

[10] *See, e.g.*, FCC, International Bureau, https://www.fcc.gov/international. While serving as Special Assistant to the Director, the FCC's Office of International Communications, the predecessor to the FCC's International Bureau, I was appointed Vice-Chair of the United States delegation to the International Telecommunications Union 1994 World Telecommunications Development Conference.

[11] FCC *Internet Freedom NPRM*, *supra* note 1, at ¶ 100.

proposes no legal basis or jurisdiction sufficient to protect Internet users from degradation, blocking, throttling, or diminished service. The FCC *Internet Freedom NPRM* questions the need for a rule prohibiting paid prioritization for Internet content, but proposes no limits on who could buy Internet priority. Neither does the FCC propose that prioritization deals should not harm other Internet users. The FCC omits analysis of the prospect that foreign entities or agents could use Internet priority to drown out U.S. voices including those of our government, military, citizens, and residents. Neither does the FCC analyze the effects of its proposals on national security or democracy. These omissions constitute arbitrary and capricious decision-making.

White House press secretary Sarah Huckabee Sanders stated on behalf of the White House: "We support the FCC chair's efforts to review and consider rolling back these rules and believe that the best way to get fair rules for everyone is for Congress to take action and create regulatory and economic certainty."[12] This "repeal without replace" proposal would eliminate the FCC's authority to respond to complaints about threats to the Internet's openness.

The FCCs *Internet Freedom NPRM* must be rejected. The FCC should withdraw the Internet Freedom NPRM in light of the FCC's arbitrary and capricious conduct of this proceeding. As discussed in this Reply Comment, the NPRM fails to analyze important issues such as the impact of its proposals on democracy and national security, to consider or provide evidence of complaints submitted to the FCC about violations of the 2015 Open Internet Order, or to analyze in detail the 2015 Open Internet Order including the record about the gatekeeper role of ISPs and its effect on edge providers. These issues must be addressed before any decision can be reached on the merits.

After conducting a proceeding compliant with the APA requirements for notice of the proposals under consideration, analysis of the relevant record, and protections to safeguard the integrity of the comment process, the FCC should retain the jurisdictional basis over ISPs under Title II of the Communications Act of 1934. Courts have recognized that Title II creates enforceable rules to prevent ISP Internet discrimination and enable the Commission to provide redress for complaints.[13] The D.C. Circuit's decision in *Verizon v. FCC, 740 F.3d 623, 655-656 (D.C. Cir. 2014)* indicates that only the Title II classification of ISPs, nor Title I or unenforceable principles, can be used to support FCC rules or jurisdiction to respond to complaints about Internet openness. That jurisdiction and those bright line rules should be maintained and the FCC should withdraw its ill-conceived 2017 *Internet Freedom NPRM*.

---

[12] Brian Fung, *The White House just endorsed the FCC's efforts to rollback its net neutrality rules*, THE WASHINGTON POST, July 18, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/07/18/the-white-house-just-endorsed-the-fccs-effort-to-roll-back-its-net-neutrality-rules/?utm_term=.2d5f7f1129ae.

[13] *Verizon v. FCC*, 740 F.3d 623, 655-656 (D.C. Cir. 2014); *United States Telecom Association (USTA) v. FCC*, 825 F.3d 674, 707 (D.C. Cir. 2016) (upholding the FCC's classification of ISPs as "common carriers" under Title II "[I]n light of *Verizon*," since as the Commission explained, "absent a classification of broadband providers as providing a 'telecommunications service,' the Commission could only rely on section 706 to put in place open Internet protections that steered clear of regulating broadband providers as common carriers *per se*."); *Id.*, at 713 (upholding the FCC's Title II classification on the grounds that "[t]he problem in *Verizon* was not that the Commission had misclassified the service between carriers and edge providers but that the Commission had failed to classify broadband service as a Title II service at all. The Commission overcame this problem in the Order by reclassifying broadband service—and the interconnection arrangements necessary to provide it—as a telecommunications service.")

II. Material False Statements Filed in the FCC *Internet Freedom* Proceeding Violate Federal and State Law and Constitute Arbitrary and Capricious Decision-making.

A. Materially False Filings Based on Identity Theft and Database Breaches in the FCC Internet Freedom Rulemaking Violate APA Standards

In the FCC's *Internet Freedom* rulemaking, twenty-seven people alleged in a May 25, 2017 letter from Fight for the Future to the FCC that their identities were stolen to file comments in the FCC Open Internet proceeding without their authorization. A copy of that letter is attached as Exhibit A.[14] The letter states "Whoever is behind this stole our names and addresses, publicly exposed our private information without our permission, and used our identities to file a political statement we did not sign onto. Hundreds of thousands of other Americans may have been victimized too."[15] The signatories requested that the FCC take down those false comments and investigate. Those complainants and identity theft victims come from 14 states as identified by their signatures on the Fight for the Future letter: 9 in California, 3 in New York, 3 in Massachusetts, 2 in Michigan, and 1 in each of Delaware, Colorado, Florida, New Hampshire, Washington, Maine, Illinois, Pennsylvania, Texas, and Utah.

Those alleged false filings are listed by the FCC's Electronic Comments Filing System (ECFS) as received by the FCC between May 8 and May 11 prior to the FCC's adoption of the *Internet Freedom NPRM*. Those filings use the same or substantially similar language:

> "The unprecedented regulatory power the Obama Administration imposed on the internet is smothering innovation, damaging the American economy and obstructing job creation. I urge the Federal Communications Commission to end the bureaucratic regulatory overreach of the internet known as Title II and restore the bipartisan light-touch regulatory consensus that enabled the internet to flourish for more than 20 years. The plan currently under consideration at the FCC to repeal Obama's Title II power grab is a positive step forward and will help to promote a truly free and open internet for everyone."[16]

This is the same text THE VERGE and ZDNet highlighted in articles reporting about unauthorized comments filed before the *Internet Freedom NPRM* was adopted.[17] ZDNet reported the

---

[14] *False Filing Victim Letter to the FCC, supra* note 2.

[15] *Id.*

[16] *See, e.g.*, comment attributed to a signatory to the False Filing Victim letter to the FCC, May 11, 2017, [search ECFS, insert under specific filing 17-108, insert in full text box the name of the identity theft victim, in the box marked express comments check yes]; Zack Whittaker, *Anti Net Neutrality Spammers are Flooding the FCC's Pages with Fake Comments*, ZDNET, May 10, 2017 ("more than 128,000 identical comments have been posted since the feedback doors were opened"), http://www.zdnet.com/article/a-bot-is-flooding-the-fccs-website-with-fake-anti-net-neutrality-comments/. I conducted a search of ECFS for the alleged false filing for each person who signed the Fight for the future letter as described in note 5. Results of that search are on file with the author and are not submitted with this Reply Comment as the FCC comment system continues as of August 29 to display names and home addresses of many of the identity theft victims as detailed in note 5.

[17] Colin Lecher, Adi Robertson, Russell Brandom, *Anti-Net Neutrality Spammers are Impersonating Real People to Flood FCC Comments*, THE VERGE, May 10, 2017 ("people contacted by *The Verge* said they did not write the comments and have no idea where the posts came from." Reporting "I have no idea where that came from," says

"comments follow the same pattern: The bot appears to cycle through names in an alphabetical order, leaving the person's name, postal address, and zip code."[18] My search of the FCC's ECFS on August 6, 2017 yielded an FCC report of 818,870 comments filed in the *Internet Freedom* proceeding with the same language listed above.

The FCC has publicly committed to investigate or take steps to prevent falsified comments using stolen identities. The letter signatories state they "are disturbed by reports that indicate you [Acting FCC Chairman Pai] have no plans to remove these fraudulent comments from the public docket."[19] They add, "[w]hile it may be convenient for you to ignore this, given that it was done in an attempt to support your position, it cannot be the case that the FCC moves forward on such a major public debate without properly investigating this known attack."[20]

Another apparent victim, Ryan Clayton, complained "[s]omeone previously submitted a comment against "net neutrality" in my name, against my wishes and without my permission," and requested that the FCC "remove fraudulently posted comments in my name from the record, which includes any that used my name and stated opposition to "net neutrality.""[21] Others expressed dismay about the *Internet Freedom* proceeding observing, "[y]es, they committed identity theft in order to prove a point."[22]

Karl Bode, a technology writer, complained to the FCC that someone filed comments without his authorization using his name and address to falsely attribute to him support for repealing the 2015 Open Internet rules.[23] Mr. Bode requested that the FCC remove comments filed without his authorization.

G. Patrick Webre, FCC Acting Chief of Government and Consumer Affairs, stated in response to Mr. Bode's request that "the FCC does not condone anyone impersonating someone else's identity."[24] Mr. Webre's letter declined the request to remove the allegedly false filing and encouraged Mr. Bode to file a comment clarifying his position and stating that the prior comment filed in his name without his authorization is false. "Once filed in the FCC's

---

Lynn Vesely, whose Indiana address also appeared, and who was surprised to hear about the comment."); Whittaker, *supra* note 16.

[18] Whittaker, *supra* note 16 (reporting that "We reached out to two-dozen people by phone, and we left voicemails when nobody picked up. A couple of people late Tuesday called back and confirmed that they had not left any messages on the FCC's website. One of the returning callers specifically said they didn't know what net neutrality was, and a third person reached in a Facebook message Tuesday also confirmed that they had not left any comments on any website.") Id., (reporting "The bot is likely automatically filing the comments through the FCC's public comment system API, which allows anyone with a free-to-obtain API key to automatically submit comments. But we don't know where the bot got its names and addresses -- though we suspect it may be from public voter registration records or an older data breach.")

[19] *False Filing Victim Letter to the FCC, supra* note 2.

[20] *Id.*

[21] Ryan Clayton, Express Comments, *supra* note 4.

[22] Tyler Barbarino, Express Comments, July 25, 2017, https://www.fcc.gov/ecfs/filing/1072130653929; *See also*, Express Comments of Benjamin Scherer, June 6, 2017, (complaining that "you [the FCC] also allow fake comments, where peoples [sic] names are used against their will, thats [sic] identity theft, and it's very serious."), https://www.fcc.gov/ecfs/filing/10606710320715.

[23] Bode, *supra* note 3.

[24] Letter from G. Patrick Webre, FCC Acting Chief of Government and Consumer Affairs, to Karl Bode, DSL Reports (July 10, 2017), https://assets.documentcloud.org/documents/3891550/FCC.pdf.

rulemaking record, there are limits on the agency's ability to delete, change, or otherwise remove comments from the record,"[25] according to Webre's letter. "Doing so could undermine the FCC's ability to carry out its legal obligation, which is to respond to all significant issues raised in the proceeding,"[26] Webre emphasized.

The FCC has offered no legal basis for its claim that limits on the agency's rulemaking process prohibit it from taking down allegedly falsified comments displaying the names and addresses of identity theft victims. Neither has the FCC proffered a legal reason that would prohibit it from masking the names and addresses of those who claim that comments were falsely filed in their names without their permission. Mr. Webre's letter does not explain how it will respond to "all significant issues raised in the proceeding" when some filings that purport to raise or address an issue constitute false statements under 18 U.S.C. 1001 and violate state identity theft laws. The FCC has announced no plans to determine the source of the alleged false filings or method to distinguish authorized from false filings based on identity theft or data breaches.

FORBES reported on the FCC's response to the victims' request to remove from public view the *Internet Freedom* comments filed without authorization. An FCC spokesperson for Chairman Pai said "[w]e will make our decision based on the facts that are in the record and on the relevant law that is presented – and obviously fake comments such as the ones submitted last week by the Flash, Batman, Wonder Woman, Aquaman and Superman are not going to dramatically impact our deliberations on this issue." Chairman Pai also emphasized that comments were filed in his name,[27] and that in the 2014-15 Open Internet proceeding comments were filed "under names like Donald Duck, Mickey Mouse, and Stalin."[28]

Chairman Pai's remarks do not recognize the important distinction between comments filed in the name of a comic book character and those filed based on stolen identities. While the trademark holder may have concerns about the use of its trade name in a public proceeding, allegations of identity theft and false federal filings are criminal in nature. False filings based on stolen identities are neither anonymous speech,[29] nor protected speech; they constitute federal and state crimes. No "Aquaman defense" absolves identity theft or false federal statements on the theory that other people filed comments in the name of a cartoon character in an attempt to be anonymous. The 27 people named in the above-cited letter to the FCC who asked the Commission to remove the false comments filed in their names are not public figures. Nor are they cartoon characters or avatars. These real people are identity-theft victims. The FCC's inaction perpetuates these crimes through the ongoing display of the names and addresses of the complainants whose names were used to make false, unauthorized filings.

In the wake of press reports about false filings that seek to manipulate the FCC's rulemaking, Chairman Pai recited on YouTube "mean tweets" taken from offensive and even

[25] *Id.*
[26] *Id.*
[27] Tony Bradley, *Victims Demand FCC Remove Fake Anti-Net Neutrality Comments*, FORBES, May 26, 2017, https://www.forbes.com/sites/tonybradley/2017/05/26/victims-demand-fcc-remove-fake-anti-net-neutrality-comments/2/#61fc72996a2a.
[28] *Id.*
[29] *See Talley v. California*, 362 U.S. 60 (1960) (ordinance requiring leafleters to fully identify themselves abridged freedom of speech as the ability speak anonymously furthers freedom of expression).

racist comments filed about his views in the *Internet Freedom* proceeding.[30] I agree that the debate in this and every governmental proceeding should be civil and that racist comments have no place in this discussion. At the same time, all must agree that identity theft and filing false statements are criminal and cannot be tolerated in federal or state rulemaking.

Rather than publicly condemn the filing of false statements using stolen identities or commit to investigate these allegations, Chairman Pai said, "[n]ow there's obviously a tension between having open process where it's easy to comment and preventing questionable comments from being filed, and generally speaking, this agency has erred on the side of openness, we want to encourage people to participate in as easy an accessible a way as possible."[31] Allowing the FCC comment system to be used as a platform for filing false material statements through identity theft is not "openness;" instead, it sanctions criminal conduct.

The FCC's comment process allows for and even encourages batch filing, and permits a person or entity to file comments on behalf of others.[32] Batch filings, even those submitted in an automated fashion, must be distinguished from false statements. Filings submitted without the authorization of the named filer abuse and manipulate the government's decision-making process. The FCC must make it clear that the comment process does not permit filings without the express authorization of the person or organization named in the comments including those submitted through the Express Comment channel.

The FCC's Chief Information Officer (CIO), David Bray, stated that the Commission doesn't use "Captcha" recognition or similar techniques that would limit filling to humans and not bots because it believes "Captcha" would hinder the access of disabled persons to FCC filing.[33] The FCC must promote access to its comment system for all Americans including those with disabilities *and* take steps to ensure that comments are filed with the authorization of the person in whose name the comment is submitted. The FCC could deter false filings by using a check box or similar indicator on the filing screen to require affirmation that the filer has the authority to file comments on behalf of the named person. The FCC's "Submit a Filing" screen only advises – "Note: You are filing a document into an official FCC proceeding. All information submitted, including names and addresses, will be publicly available via the web."[34] That advisory is inadequate. Instead, the FCC should display a note informing filers that

---

[30] See, John Eggerton, *FCC's Pai Reads Mean Tweets*, BROADCASTING AND CABLE, May 15, 2017, http://www.broadcastingcable.com/news/washington/fccs-pai-reads-mean-tweets/165811.

[31] *Id.*

[32] FCC, Restoring Internet Freedom Comments, https://www.fcc.gov/restoring-internet-freedom-comments-wc-docket-no-17-108 ("We strongly encourage parties who seek to file a large number of comments or "group" comments to do so through the public API…As another option, parties may make use of this Restoring Internet Freedom ECFS Bulk Upload Template (below) to upload a CSV file. We ask commenters to be patient, as there may be some lag time between when filings are made and when they appear in ECFS. All timely and properly formatted filings will be part of the record in this proceeding.")

[33] Michael Krigsman, *CIO Diary: Lessons from the FCC Bot-Swarm Attack,* ZD NET, May 19, 2017 (citing statement by FCC CIO David Bray that the FCC Electronic Comments Filing System (ECFS) is "open by design." "The emphasis on data accessibility also means that spam fighting systems, like CAPTCHA, are not an option because they may interfere with access from legitimate users. For example, these tools can stop some users, who may possess disabilities, from accessing the site. Importantly, public stakeholders also want to allow users to submit comments on behalf of others using automation.), http://www.zdnet.com/article/cio-diary-lessons-from-the-fcc-bot-swarm/.

[34] FCC, Submit a Filing, https://www.fcc.gov/ecfs/filings.

submission constitutes the filer's certification under penalty of perjury that the filer is authorized to submit the material on behalf of the named commenter. Such notice would deter false statements based on identity theft and database breaches.

The alleged false filings based on identity theft must be examined in the context of allegations of a "bot swarm"[35] and the FCC's report to Congress that a "non-traditional" Distributed Denial of Service (DDoS) attack afflicted the FCC's comment system.[36] The FCC reported to Congress that a "bot swarm"[37] peaking at 30,000 requests per minute overwhelmed the FCC's comment system from May 7-8, 2017 and "effectively blocked or denied additional web traffic-human or otherwise-to the comment filing system."[38] The FCC's CIO reported that "the attack did not come from a botnet of infected computers but was fully cloud-based."[39] May 8th was the first date of the submission to the FCC of the alleged false filings cited in the Fight for the Future letter from the 27 signatories. Senators Schatz, Leahy, Franken, Markey, and Wyden wrote to Acting FBI Director McCabe on May 31, 2017, asking for an investigation into the DDoS attack the FCC initially claimed afflicted its comment system.

The FCC reported to Congress that the Commission's IT staff "found other markers of potential malicious intent."[40] Chairman Pai's June 15, 2017 response letter states that bots sought to access the FCC's application programming interface (API), which the FCC makes available for bulk filings "not to submit comments, but merely to create an artificial demand for additional resources on the cloud-based system. This appears to have been designed to impede the performance of the comment filing system's components."[41] The FCC's letter states that the FCC Chief Information Officer spoke with the FBI, and "the conclusion was reached that, given the facts currently known, the attack did not appear to rise to the level of a major incident that would trigger further FBI involvement. The FCC and FBI agreed to have further discussions if additional events or the discovery of additional evidence warrant consultation."[42] The FCC's June 15th letter to Senators Schatz, Leahy, Franken, Markey, and Wyden did not address allegations of identity theft or data breaches in this proceeding.

In reply several members of Congress questioned the Commission's cybersecurity procedures. They expressed concerns about "reports of as many as 150,000 comments that

---

[35] Krigsman, *supra* note 33 ("By using commercial cloud services to make massive API requests, the bots consumed available machine resources, which crowded out human commenters. In effect, the bot swarm created a distributed denial of service attack on FCC systems using the public API as a vehicle.")

[36] Letter from Ajit Pai, Chairman FCC, to Senator Ron Wyden, June 15, 2017, Attachment, 1, [hereinafter *FCC Chair Pai letter to Senator Wyden*], http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0627/DOC-345556A1.pdf.

[37] See Krigman, *supra* note 33 (according to FCC CIO Bray, "FCC staff noticed high comment volumes around 3:00 AM the morning of Monday, May 8. As the FCC analyzed the log files, it became clear that non-human bots created these comments automatically by making calls to the FCC's API.").

[38] *FCC Chair Pai letter to Senator Wyden*, *supra* note 36.

[39] Krigsman, *supra* note 33. *See*, Search Security, Tech Target (defining a botnet as "a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware. Users are often unaware of a botnet infecting their system."), http://searchsecurity.techtarget.com/definition/botnet.

[40] *FCC Chair Pai letter to Senator Wyden*, *supra* note 36.

[41] *Id.*

[42] *Id.*

disappeared from the FCC's net neutrality docket," and that "automated comments were submitted to the FCC using names and addresses of real people without their knowledge or consent."[43] The letter asked the FCC "to examine these serious problems and irregularities that raise doubts about the fairness, and perhaps even the legitimacy, of the FCC's process in its net neutrality proceeding."[44]

The FCC's failure to commit to investigate the sources of the "bot swarm" that it characterized as "designed to impede the performance of the comment filing system's components"[45] is egregious, particularly in light of the allegations of false filings based on identity theft and data breaches, many of which appear to have been filed by bots in light of their alphabetical and rapid filings. These failures reflect arbitrary and capricious decision-making in violation of the APA, and a miscarriage of the FCC's public duties.

Congressman Pallone requested that the U.S. Department of Justice (US DOJ) and the FBI investigate allegedly false filings in the *Internet Freedom* proceeding, including filings that may have been derived from one or more data breaches. Congressman Pallone's June 28, 2017 letter to Attorney General Jefferson Sessions and Acting Director of the FBI, Andrew McCabe, attached as Exhibit B, highlights the filing of more than 450,000 identically worded comments filed by an unidentified party, as well as allegations that some of the falsified comments may be "using information obtained from data breaches."[46] Congressman Pallone expressed concern that "the sheer number of these potentially false comments suggest a coordinated attempt to materially mislead the FCC, and therefore a coordinated attempt to break federal law."[47]

I concur with the requests of Senators Schatz, Leahy, Franken, Markey, and Wyden and Congressman Pallone that the DOJ and the FBI investigate the allegedly false statements and the bot attacks in the FCC *Internet Freedom* rulemaking. The FCC reported that it does not release its server logs in response to Freedom of Information Act requests "because they might contain private information such as IP addresses."[48] This is a spurious response; the FCC could, instead, redact "private information" from server logs and then produce them. In addition, state and federal law enforcement officials should deploy investigative tools such as subpoenas, discovery requests, and grand juries to determine who is responsible for any false filings based on identity theft or data breaches. Law enforcement authorities must also determine whether those responsible for the false filings based on identity theft or database breaches are domestic or foreign actors or agents. The hacking of voter registration data from 39 states in 2016 raises the

[43] *Congressional letter to FCC re: bot attacks and false filings based on data breaches, supra* n. 3.
[44] *Id.*
[45] *Id.*
[46] Letter from Congressman Frank Pallone to the Honorable Jefferson B. Sessions III, Attorney General, and Mr. Andrew McCabe, Acting Director, FBI, June 28, 2017, https://democrats-energycommerce.house.gov/newsroom/press-releases/pallone-to-justice-department-fbi-investigate-fake-fcc-net-neutrality-docket (citing Colin Lecher, Russell Brandom, Adi Robertson, *The Anti Net Neutrality Bot Spamming the FCC is Pulling Names from Leaked Databases*, THE VERGE, May 11, 2017). See also Whittaker, *supra* note 16.
[47] *Id.*
[48] Zach Whittaker, *FCC Won't Publish Evidence of DDoS Attack, Amid Net Neutrality Debate, The agency has "gigabytes" of server logs that offer evidence for the alleged distributed denial-of-service-attack, but it won't make them public*, ZDNET, May 21, 2017, ZDNet, http://www.zdnet.com/article/fcc-will-not-publish-evidence-of-alleged-ddos-attack/.

prospect that voter data may be misused as a source to manipulate government decision-making and perpetrate identity theft.[49]

False filing allegations raise additional alarm bells in light of Congressional findings of a Russian influence campaign in 2016 aimed at the United States presidential election, findings incorporated into the *Countering America's Adversaries Through Sanctions Act*.[50] The Oxford Internet Institute identified and analyzed "Cyber troops," "government, military or political party teams committed to manipulating public opinion over social media."[51] Malicious bots have been deployed in several countries in an attempt to sway public opinion. During the 2017 French presidential elections "cyber troops" unleashed bots "to falsely popularize political issues during high-profile campaigns to give the impression of a groundswell of grassroots support."[52]

In addition to federal investigations, state Attorneys General should investigate and prosecute under state law the identity theft crimes perpetrated in the *Internet Freedom* proceedings. As discussed below, the false filings in the *Internet Freedom* rulemaking constitute a *prima facie* case of identity theft under state laws such as California Penal Code 530.5, aggravated identity theft under 18 U.S.C.1028(a)(7), as well as violations of 18 USC 1001.

This investigation and prosecution should be a high priority for states home to identity theft victims in the *Internet Freedom* proceeding, states and those who submitted comments in this rulemaking, and for all Americans. The FCC's Internet rules affect all states, businesses, democratic institutions, and national security. State, local, and tribal governments, residents, businesses, education, emergency services agencies, health care, critical infrastructure[53] and civic

---

[49] *See. e.g.*, Michael Riley and Jordan Robinson, *Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known*, BLOOMBERG POLITICS, June 13, 2017 (reporting that Russian hackers intruded voter data bases in 39 states during the 2016 election season. "In Illinois, investigators found evidence that cyber intruders tried to delete or alter voter data."), https://www.bloomberg.com/amp/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections; Threat Intelligence Blog, *Data Breach Alert: 40 Million U.S. Voter Records for Sale*, LOOKING GLASS, July 31, 2017 ("Over the past few weeks, LookingGlass Cyber Solutions has tracked in an underground forum, the leak of nearly 40 million U.S. voter records from eight different states. The stolen data contains the personal and sensitive information of current and former voters from the following states": Arkansas, Colorado, Connecticut, Delaware, Florida, Ohio, Oklahoma, Michigan. "The threat actor "Logan" advertised this information for sale on RaidForums, and is intimating that he/she may possess as many as 20-25 additional state voter databases."), https://www.lookingglasscyber.com/blog/threat-intelligence-insights/data-breach-alert-9-states-voter-databases-sale/.

[50] *Countering America's Adversaries Through Sanctions Act*, *supra* note 9, Title II, § 211.

[51] Samantha Bradshaw, Philip N. Howard, *Troops, Trolls, and Troublemakers: A Global Inventory of Organized Social Media Manipulation* (Oxford Internet Institute, Computational Propaganda Research Project, Working Paper No. 2017.12), http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf.

[52] April Glaser, *Twitter Bots are Being Weaponized to Spread Information on the French Presidential Campaign Hack, 5 Percent of the Accounts Tweeting #MacronGate Make up 40 percent of the Tweets*, RECODE, May 6, 2017, https://www.recode.net/2017/5/6/15568582/twitter-bots-macron-french-presidential-candidates-hacked-emails.

[53] Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195(e) (2001)(defining "critical infrastructure" as "means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."); The White House, Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21) (Feb. 12, 2013) (designating 16 sectors as "Critical Infrastructure:" Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense-Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government

institutions including elections are profoundly affected by the FCC's Open Internet rules and the process through which those rules are considered. All of us will be affected by the lack of any enforceable rules protecting Internet openness if the FCC adopts its "lead proposal" [54] to reclassify ISPs as information service providers and remove the legal footing for enforcement or complaint jurisdiction. The alleged false filings attempt to infect the FCC's decision-making process. The FCC has reacted with indifference to these false filing and identity theft allegations and has failed to commit to root out and stop this conduct.

False filings based on identity theft hack the tools of democratic decision-making for an ulterior motive. This criminal conduct – whether perpetrated by domestic or foreign actors or their agents – strikes at the heart of American democracy. Those responsible must be identified and held to account for their criminal activity. The FCC, the federal government, the states, and all Americans must stand for the integrity of our governmental decision-making process.

The FCC must cooperate with federal and state investigations into the unlawful manipulation of its comment process. The FCC and State Attorneys General must take immediate steps to protect the victims of identity theft in the FCC *Internet Freedom* proceeding. As discussed below, the FCC's failure to address the false filings, identity theft, and use of information obtained through data breaches in this proceeding constitutes arbitrary and capricious decision-making under the APA. The FCC must investigate and address these allegations of criminal conduct in the *Internet Freedom* rulemaking process before it can consider any proposal on the merits. The FCC should pause the Internet Freedom rulemaking to investigate these allegations and withdraw the Internet Freedom NPRM in light of these unprecedented attacks on the proceeding's integrity, and the proposals deficiencies as discussed in sections III and IV of this Reply Comment.

B. Submitting a False Federal Statement Based on Stolen or Misappropriated Information Constitutes Identity Theft Under State Law in California and other Jurisdictions, and a Federal Crime

Federal law prohibits making any materially false statement or representation in any matter within the jurisdiction of an executive, legislative, or judicial branch. 18 USC 1001. Filing comments in a federal proceeding by misappropriating the identity of another person who does not authorize that filing constitutes a *prima facie* case of federal and state law identity theft and false statement crimes. This conduct may also raise civil claims.

To substantiate a false statement claim under 18 USC 1001, the government must prove five elements beyond a reasonable doubt: (1) a statement, (2) falsity, (3) materiality, (4) specific intent, and (5) agency jurisdiction.[55] A filing submitted to the FCC's comment system is a statement under the statute. Falsity would be shown by submitting a filing without the

---

Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Water; Transportation Systems; Water and Wastewater Systems), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; Dept. of Homeland Security, Critical Infrastructure Sectors, https://www.dhs.gov/critical-infrastructure-sectors.

[54] *FCC Internet Freedom NPRM*, *supra* note 1, at ¶ 100.

[55] *U.S. v. Lawson*, 809 F.2d 1514, 1517 (11th Cir. 1987).

authorization of the person named in the comments with the intent to make it appear as if it were comments of that person. To satisfy the materiality element the "false statement need not have actually influenced the agency, and the agency need not rely on the information in fact for it to be material."[56] The weight the FCC may ultimately give in the *Internet Freedom* proceeding to the allegedly materially false statements based on stolen identities does not influence their materiality. "A material fact is one that has a natural tendency to influence or be capable of influencing the government agency or department in question.[57] Evidence of the defendant's specific intent to bring about the unlawful act satisfies the specific intent element of 18 USC 1001.[58] Possession and use of unlawfully obtained personal information to file an unauthorized statement made to appear as if it reflected the views of the identity theft victim likely satisfies the specific intent requirement. A statement is within agency jurisdiction as required by 18 USC 1001 when a department or agency has power to exercise authority in a particular situation.[59] The FCC has the power to adopt an order in the *Internet Freedom* rulemaking for which the comments were considered, and thus the statement is within the agency's jurisdiction.

Comments including Express Comments submitted through the FCC's electronic comments filing system are intended to influence the FCC's decision-making process, a factor sufficient to indicate their materiality. Such false filings also influence public opinion about the FCC rulemaking, which in turn influences the FCC's decision-making process. The FCC defines misrepresentation as a false statement of fact made with intent to deceive the Commission.[60] A comment that purports to be filed by or on behalf of a particular individual as indicated by the use of their name and home address in the comment is a statement of fact within the FCC's rules. 18 U.S.C. 1001's proscriptions against false filings in a federal matter are not limited to licensees or applicants for a license, but apply to all who submit false statements in a federal proceeding. A *prima facie* case can be made alleging violations of 18 U.S.C. 1001 arising from false statements submitted without authorization of the named filers, particularly for those names derived through identity theft including data breaches.

This conduct also appears to violate the Federal Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. 1028(a)(7), also known as Aggravated Identity Theft. That Act subjects to federal criminal penalty any person who "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[61] Crimes which trigger the Aggravated Identity Theft laws of 18 USC 1028(a) include any crime from Chapter 47 of the criminal code relating to fraud and false statements (e.g., 18 USC 1001). Under that statute the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual. 18 USC 1028 (d)(7).

---

[56] *United States v. Serv. Deli Inc*., 151 F.3d 938, 941 (9th Cir.1998); *see also United States v. King*, 735 F.3d 1098, 1108 (9th Cir. 2013).
[57] *Id.* at 1520 (citing *United States v. Baker,* 626 F.2d 512 (5th Cir.1980)).
[58] *U.S. v. Markee*, 425 F.2d 1043, 1046 (9th Cir. 1970).
[59] *United States v. Rodgers,* 466 U.S. 475, 479 (1984).
[60] *Fox River Broadcasting, Inc.,* 93 FCC 2d 127, 129 (1983) (defining misrepresentation and lack of candor by FCC licensees).
[61] 18 U.S.C. 1028(a)(7).

Obtaining and listing on a federal filing another person's name and address without that person's authorization satisfies the requirement of the use of "means of identification of another person" with the intent to commit a violation of Federal law such as a false filing under 18 USC 1001. The House Report accompanying enactment of § 1028(a) explained that it "is the view of the Committee that the intent to defraud the United States in this context is an intent to use the identification document to commit an offense against the United States, for example, an offense under 18 U.S.C. 1001 [knowing false statement to governmental agency].[62] Using purloined means of identification to file a false statement and commit identity theft under state law likely satisfies the unlawful activity element of federal Aggravated Identity Theft.

Allegations that data breaches or hacks were the source of personal identifying information used to file false statements in the *Internet Freedom* proceeding suggests violations of the Computer Fraud and Abuse Act under 18 U.S.C. § 1030(a)(2) (accessing a computer and obtaining information without authorization). That statute protects a "protected computer," which § 1030 defines as a computer used in or affecting interstate or foreign commerce or communication. A violation or attempted violation of section § 1030(a)(2) is a felony if: committed for commercial advantage or private financial gain; committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or; the value of the information obtained exceeds $5,000. Unauthorized access of a computer to commit identity theft under state law may satisfy the required elements for a felony charge under § 1030. Determining whether the perpetrator acted for commercial advantage or private financial gain, as well as the value of the information obtained will be important to evaluating a potential violation of § 1030. The use of stolen information to commit a crime of false filing or a state identity theft violation or civil tort likely satisfies the second prong of § 1030(a)(2), indicating that such violations could be charged as felonies.

The laws of several states including California make identity theft or unlawful use of personal identifying information a crime. Section 530.5(a) of the California Penal Code criminalizes "willfully obtaining another person's personal identifying information and using that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person…" Personally identifying information may include names, addresses, and several other identifiers. Cal. Penal Code 530.55.

Identity theft charges under Cal. Penal Code 530.5 require a showing that the defendant: (1) willfully obtained personal identifying information belonging to someone else; (2) used that information for any unlawful purpose; and (3) used the personal identifying information without the consent of the person whose personal identifying information is being used."[63] *People v. Valenzuela*, 205 Cal.App.4th 800, 808, recognized that the perpetrator of identity theft can 'commit other crimes by using the victim's identity, causing great harm to the victim." "[T]he retention of personal identifying information of multiple victims constitutes multiple identity theft offenses."[64] Willfully obtaining personal identifying information such as names and

[62] *In re McBride* 602 A.2d 626, 634 (D.C. 1992) (citing H.R.Rep. No. 1396, 96th Cong., 2d Sess. 14 (1980)).
[63] *People v. Valenzuela*, 205 Cal.App.4th 800, 808 (2012) (citing *In re Rolando S.*, 197 Cal.App.4th 936, 940) (2011); see also *People v. Tillotson*, 157 Cal.App.4th 517, 533 (2007).
[64] *People v. Valenzuela*, 205 Cal.App.4th 800, 808.

addresses for the unlawful purpose of committing a crime by filing a false statement under 18 USC 1001 constitutes a *prima facie* case of identity theft under California Penal Code § 530.5.

Some state identity theft laws also require that the person who stole or used the identifying information for an unlawful purpose gain a benefit from that wrongdoing.[65] Authorities must determine whether those responsible for false filings in the *Internet Freedom* rulemaking have a commercial or financial motive or received a benefit for their conduct such as payment by another party for the number of comments filed. Authorities should also investigate whether those responsible for the false filings based on misappropriated identities hope to gain financially from the policy the FCC may adopt in response to comments. The FCC and law enforcement agencies must also determine whether those who perpetrated the false filings are affiliates, agents of, or are supported by others who hope to obtain a benefit from the FCC's decision in this rulemaking.

FCC rules have consistently held parties responsible for filing false statements, misrepresentations, or lack of candor with the Commission. The FCC has investigated, fined, and even found unfit to hold a FCC license those who engage in such wrongdoing. *See, e.g.* RKO General, Inc., Decision, 78 F.C.C. 2d 1 (1980), *aff'd*, 670 F.2d 215 (D.C. Cir. 1981) (denying an application based on applicant's lack of candor in proceedings before the FCC); Pass Word, Inc., Order to Revoke Licenses, 76 F.C.C. 2d 465 (1980) ¶ 10, *aff'd*, Pass Word Inc. v. FCC, 673 F.2d 1363 (D.C. Cir. 1982) (revoking license for deliberate concealment and misrepresentations to the Commission). The FCC must take steps to affirm that no FCC licensee or its affiliates or agents are involved in any fashion in the allegedly false statements based on identity theft submitted in the *Internet Freedom* proceeding. Nor should the FCC tolerate false statements by non-licensees. False material statements in a federal proceeding are criminal, regardless of the source.

California is home to nine of the twenty-seven people from fourteen states who wrote to the FCC in the Fight for the Future letter demanding removal of the comments falsely filed under their names without their authorization in the *Internet Freedom* rulemaking.[66] Identity theft victims in the *Internet Freedom* proceeding should submit complaints to their State Attorney General and file police reports if they have not already done so. California and other states home to victims of identity theft perpetrated in the FCC *Internet Freedom* proceeding should use state authority to investigate and prosecute those responsible for these alleged crimes.

State Attorneys General should insist that the FCC take immediate steps to protect the identity theft victims including removing comments falsely attributed to them which display their names and addresses. I respectfully recommend that State Attorneys General join my call for

[65] *See*, e.g., Colorado R.S. 18–5902(1)(a) ("A person commits identity theft if he or she: (a) Knowingly uses the personal identifying information, financial identifying information, or financial device of another without permission or lawful authority with the intent to obtain cash, credit, property, services, or *any other thing of value* or to make a financial payment);" *People v. Campos* 351 P.3d 553, 555 (Colo. App. 2015); Kansas.S.A.2011 Supp. 21–6107(a) ("Identity theft is obtaining, possessing, transferring, using, selling or purchasing any personal identifying information, or document containing the same, belonging to or issued to another person, with the intent to defraud that person, or anyone else, in order to receive any benefit."); *State v. Saldana*, 353 P.3d 470 (Kan. Ct. App. 2015) (Mar. 28, 2016); National Conference of State Legislatures, *Identity Theft*, http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx.

[66] *False Filing Victim Letter to the FCC, supra* note 2.

suspension of the FCC's *Internet Freedom* proceeding to investigate these criminal allegations which undercut the integrity of the FCC's proceeding. Withdrawal of the *Internet Freedom NPRM* would also provide the FCC an opportunity to address the deficiencies in the FCC's current proposals that puts democracy, national security, and the Open Internet at risk, and fails to comply with the APA, as discussed in sections III and IV of this Reply Comment.

Chairman Pai's statements in response to the identity theft and false filing allegations[67] suggest the FCC will address the false comments through the weight it accords to comments and the record. The FCC's failure to review the scope and responsibility for allegedly false statements based on data breaches and identity theft renders the Commission incapable of determining which comments to exclude or accord less weight, or to refer to law enforcement.

ISP Industry Association Representatives CTIA, NCTA – the Internet & Television Association, and USTelecom stated in opposition to a motion to extend the Reply Comment period that "[t] he vast majority of comments filed merely state (often in one or two sentences) the commenter's ultimate policy preferences."[68] *Natural Resources Defense Council, Inc. v. U.S. E.P.A.*,[69] stated that the "number and length of comments, without more, is not germane to a court's substantial-evidence inquiry."[70] The FCC is duty bound by the APA to analyze the comments and their substantive contributions, and to investigate allegations that someone has allegedly stolen identities to "puff up" their side of the argument and submit false statements.

The D.C. Circuit cautioned the FCC in 1969 that it was not to treat a Public Intervenor like an "interloper."[71] The FCC may not dismiss or diminish public comment in its rulemaking proceeding by according public comment little weight or analysis, and failing to analyze allegations of criminal manipulation of the public comment process. The FCC has engaged in no process to separate allegedly false from authorized comments. Identifying the source of the false filings is a necessary predicate to analyzing all comments and the record in the *Internet Freedom* docket and to coming to a decision based on a record created with integrity.

The FCC has not committed to investigating the alleged false filings, though the Commission is on notice that hundreds of thousands of identical comments may have been filed without authorization of the named commenter.[72] As of August 29, 2017 15,930 people signed a petition by Fight for the Future that calls for the FCC to take the following actions: "[1] Notify

---

[67] See *supra* text accompanying notes 24-31.

[68] CTIA, NCTA – the Internet & Television Association, and USTelecom, Opposition To Motion For Extension Of Time, In the Matter of Restoring Internet Freedom, 17-108, August 10, 2017, p. 3 [hereinafter *Opposition To Motion For Extension Of Time*], https://ecfsapi.fcc.gov/file/1081083338971/CTIA%20NCTA%20USTelecom%20RIF%20Opposition%20to%20Extension.pdf.

[69] 822 F.2d 104, 122 (D.C. Cir. 1987).

[70] *Natural Resources Defense Council, Inc. v. U.S. E.P.A.*, 822 F.2d 104, 122 (*Cf. Association of Data Processing Service Organization v. Board of Governors,* 745 F.2d 677 (D.C.Cir.1984) (discussing substantial evidence review)).

[71] *Office of Communication of United Church of Christ v. F.C.C.*, 425 F.2d 543, 546 (D.C. Cir. 1969).

[72] *See, Congressional letter to FCC re: bot attacks and false filings based on data breaches*, *supra* note 3; Letter from Congress Member Pallone, *supra* note 46.

all who have been impacted by this attack, [2] remove all of the fraudulent comments, including the ones made in our names, from the public docket immediately, [3] publicly disclose any information the FCC may have about the group or person behind the 450,000+ fake comments, and [4] call for an investigation by the appropriate authorities into possible violations of 18 U.S.C. § 1001 ("Making false statements") and other relevant laws."[73] Despite calls for scrutiny of these allegedly fraudulent actions, the FCC has taken no action to remove the allegedly false filings or initiate a public investigation.

CTIA, NCTA – the Internet & Television Association, and USTelecom cited a different set of allegations of false or suspicious filings in their opposition to a motion for the FCC to extend the Reply Comment deadline. The Industry Associations argued that "[a]s widely reported, many of these comments are apparently fabricated, not associated with the actual individuals whose names appear on them (where any such name appears at all). One study revealed that over seven million of the comments filed between July 3 and August 4, 2017 appear to be entirely fraudulent.[74] The opposition of CTIA, NCTA – the Internet & Television Association, and USTelecom does not acknowledge or cite the allegations that false filings based on identity theft were submitted to allegedly support the repeal of the Open Internet rules or the letter submitted from the identity theft victims submitted by Fight for the Future. Their opposition references the National Legal and Policy Center allegations of allegedly fake comments and filings listing residences abroad including Russia.

The National Legal and Policy Center (NLPC) alleges that 5.8 million fake comments supporting net neutrality were "submitted between July 17th and July August 4th, come from one of 10 email domains associated with a fake email generator program found at http://www.fakemailgenerator.com."[75] Peter Flaherty writing for NLPC wrote that a "spot check of several of the 1.5 million of the comments filed between July 17th and August 4th showed that every address checked was invalid. Based on the analysis, NLPC believes that 95% or more of the comment addresses are using a fake address." Flaherty does not detail his methodology

[73] Fight for the Future, More than 15,000 people call on the FCC to remove and investigate fake anti-net neutrality comments using stolen names and addresses, June 12, 2017, https://www.fightforthefuture.org/news/2017-06-12-more-than-15000-people-call-on-the-fcc-to-remove/(last visited August 29, 2017); Fight for the Future, https://actionnetwork.org/petitions/tell-the-fcc-remove-fake-comments-immediately-and-call-for-an-investigation-by-the-appropriate-authorities. These people's names and addresses were stolen and used to submit fake comments against net neutrality. Tell the FCC to do something about it! , https://actionnetwork.org/petitions/tell-the-fcc-remove-fake-comments-immediately-and-call-for-an-investigation-by-the-appropriate-authorities (last visited August 29, 2017).

[74] *Opposition To Motion For Extension Of Time*, *supra* note 68, at 3, n. 10 (citing Peter Flaherty, *Another 5.8 Million Fake Net Neutrality Comments Found*, Nat'l Legal and Policy Ctr. (Aug. 8, 2017), http://nlpc.org/2017/08/08/another-5-8-million-fake-net-neutralitycomments-found-1-5-million-fakes-put-online-public-scrutiny/ (detailing 5.8 million fake comments filed between July 17, 2017 and August 4, 2017); Peter Flaherty, *Analysis: 1.3 Million More Pro-Net Neutrality FCC Public Comments Came From Russia, Other Foreign Countries*, Nat'l Legal and Policy Ctr. (July 17, 2017) (detailing 1.3 million fake comments filed between July 3, 2017 and July 12, 2017 alone, from "addresses in France, Russia and Germany")),], https://ecfsapi.fcc.gov/file/1081083338971/CTIA%20NCTA%20USTelecom%20RIF%20Opposition%20to%20Extension.pdf.

[75] Peter Flaherty, *Another 5.8 Million Fake Net Neutrality Comments Found; 1.5 Million Fakes Put Online for Public Scrutiny*, National Legal and Policy Center, June 7, 2017, https://nlpc.org/2017/08/08/another-5-8-million-fake-net-neutrality-comments-found-1-5-million-fakes-put-online-public-scrutiny/.

that led to his conclusion that 5.8 million allegedly fake comments were filed in this manner. NLPC called for an investigation into the comment filing process stating "[s]omeone or some group is making a complete mockery of our public rulemaking process."[76]

The major ISP Industry Associations in the Opposition to the Motion to extend time to file Reply Comments do not call for an investigation into the allegedly fake comments but instead argue that "Moreover, all parties have had adequate time to consider their arguments in the current rulemaking."[77] Falsified statements submitted under the pretense that they were filed by someone whose name and address were stolen in an attempt to support an argument about what the FCC should or should not do does not reflect parties' consideration of the arguments. Identity theft victims did not authorize falsified comments filed in their names. The record reflects falsity not consideration of arguments.

The FCC has manifested a bewildering indifference to these serious allegations of criminal conduct. The FCC's Order extending time to file Reply Comments acknowledged that "Opponents [to the motion to extend time] also assert that the "vast majority of comments filed merely state (often in one or two sentences) the commenter's ultimate policy preferences," and that "many of these comments are apparently fabricated." In support of these assertions, Opponents state that "[o]ne study revealed that over seven million of the comments filed between July 3 and August 4, 2017 appear to be entirely fraudulent."[78] The Reply Comment deadline extension Order, the letter submitted to the FCC by victims alleging identity theft in the *Internet Freedom* proceeding, and the response by FCC Chairman Pai to the identify theft allegations all show that the FCC is aware of these serious allegations. These responses evidence the FCC's failure to committ to investigate these allegations or pause its proceeding to coordinate with state and federal authorities to investigate allegations of criminal conduct in this proceeding that undercut the integrity of the Commission's rulemaking process.

The FCC granted a two week extension for submission of Reply Comments "to provide parties additional time to analyze the legal, and policy arguments raised by initial commenters," citing cable and Lifeline proceedings where the FCC granted extensions to develop the record or allow for thoughtful consideration of the issues.[79] The "business as usual" rationale for granting

---

[76] *Id.*
[77] *Id.*
[78] FCC, Wireline Competition Bureau, Order, Aug. 11, 2017, Docket No. 17-108, https://ecfsapi.fcc.gov/file/0811285508250/DA-17-761A1.pdf.
[79] Id., p. 2, n. 9 (citing *See, e.g., Promoting Innovation and Competition in the Provision of Multichannel video programming distribution services*, MB Docket No. 14-261, Order, 30 FCC Rcd 1160 (MB Feb. 10, 2015) (granting a two-week extension of the comment and reply deadlines after parties sought a longer extension); *Wireless Telecommunications Bureau Extends Period to File Reply Comments on Motorola, Inc. Request for Interpretation or Waiver of Section 90.267 of the Commission's Rules Regarding 450-470 MHz Band Low Power Operators*, WT Docket No. 10-74, Public Notice, 25 FCC Rcd 4694 (MB May 3, 2010) (granting a 10-day extension of reply comment deadline upon motion for a longer extension, "to ensure that the Commission obtains a complete and thorough record"); *Lifeline and Linkup Reform and Modernization*, WC Docket Nos. 11-42, 09-197, 10-90, Order, 30 FCC Rcd 8233 (WCB Aug. 5,2015) (granting two-week extensions for filing comments and replies, finding that limited extensions "will allow for more thoughtful consideration of the issues raised . . . , while at the same time not unduly delaying the resolution of these issues"); *Cable Television Technical and Operation Requirements*, MB Docket No. 12-217, Order, 27 FCC Rcd 16019, (MB Dec. 21, 2012) (granting a two-week extension, given the importance of the issues, when parties sought a longer extension)."

the extension is at odds with the acknowledgment of the opponents arguments that false comments were filed and with the prior notice to the FCC that identity theft was being conducted to submit false comments in this proceeding. The FCC ordered the extension based on its finding that "permitting interested parties an additional two weeks in which to file their reply comments will allow parties to provide the Commission with more thorough comments, ensuring that the Commission has a complete record on which to develop its decisions." The FCC fails to acknowledge that without the agency releasing the "url" information and source information about filings or the alleged bot swarm, parties cannot on their own develop a complete record about the conduct of this proceeding and the implications of the FCC's proposals for constraint of Internet access or protection against degradation of service by those favored by the FCC's proposals. Neither can the FCC develop a complete record without investigating these allegations. Missing from the FCC's extension order, the statements by Chairman Pai, and FCC spokespersons is the sense of urgency or expression of concern that the FCC process is being manipulated by criminals and that this conduct demands law enforcement investigation.

The FCC, like all federal agencies, must allow a meaningful opportunity for public comment and is on notice from several identity theft victims and from many participants in this proceeding that its comment process is being manipulated to criminal ends. The D.C. Circuit observed in *Office of Communications of the United Church of Christ v. FCC* that "A curious neutrality-in-favor-of-the-licensee seems to have guided the Examiner in his conduct of the evidentiary hearing."[80] Likewise, the FCC is curiously neutral and unmoved about allegations of identity theft, false filings, and a bot swarm that allegedly took down their comment filing system.[81] The FCC did not ring alarm bells or pause the proceeding to investigate these issues as the FCC frequently does when merger reviews, for example, require additional analysis and the FCC "stops the clock." Instead, the FCC granted a business-as-usual two week extension for filing Reply Comments, signaling its intention to continue to proceeding without a hiatus to investigate these unprecedented allegations of criminal conduct perpetrated in its rulemaking process. The FCC must pause the proceeding and investigate these serious criminal allegations which impair the rulemaking process.

As a former Director of the FCC's Office of Communications Business Opportunity, a former member of the Federal-State Joint Conference on Advances Services, a former Commissioner of the California Public Utilities Commission, a law professor, and a citizen I am baffled at the FCC's failure to stand up for the integrity of its rulemaking process. The FCC needs to recognize that criminals are manipulating the system for FCC decision-making, and announce that it will not tolerate such criminal conduct. Instead, the FCC granted a two-week extension and continues to march this proceeding along like it is business as usual. The FCC needs to stand up for the integrity of its process to protect the American public, participatory democracy through notice-and-comment rulemaking under the APA, and to stop criminal conduct. The FCC cannot address these issues by adjusting the weigh afforded to public comment without analyzing which are false and which are authentic, and who is behind the manipulation of the FCC's decision-making process.

[80] *Office of Communication of United Church of Christ v. F.C.C.*, 425 F.2d 543, 547.
[81] *Supra* note 27-42 and accompanying text.

Public comments, including those filed as Express Comments are part of the FCC record, and the FCC has accorded them weight in past proceedings including the 2015 Open Internet Order.[82] Executive Order 13,579 adopted in 2011 provides that regulatory "decisions are informed and improved by allowing interested members of the public to have a meaningful opportunity to participate in rulemaking."[83] While now listed on the White House website as "historical material frozen in time,"[84] President Trump has not issued an Executive Order rescinding the presidential directive to encourage public participation and comment in federal rulemakings.

The FCC's Open Internet order treated public comment as a source of information and analysis of the agency's proposal, not merely as an exercise in public participation in FCC decision-making. Lauren Moxley observed that in compiling Comment Summaries for the 2015 Open Internet proceeding the FCC was "focusing resources on substantive long-form comments, paying special attention to middle-ground comments that conveyed valuable first-person experiences, and formulating final rules based on information gleaned in the process, the FCC seemed to consider the public comments not solely as an opinion poll, but as a method to learn more from the public about the potential effects of the proposed rules.[85]

The Code of Federal Regulations 47 C.F.R. 1.21(a) states that "Any party may appear before the Commission and be heard in person or by attorney." That rule allows public appearance before the FCC and reflects the FCC's duty to hear the subject of that appearance. 47 C.F.R. 1.400 defines the "party" as a reference "to any person who participates in a proceeding by the timely filing of a petition for rule making, comments on a notice of proposed rule making, a petition for reconsideration, or responsive pleadings in the manner prescribed by this subpart. The term does not include those who submit letters, telegrams or other informal materials." Comments filed through the FCC's Express Comment category are not labeled by the FCC website as "letters, telegrams or other informal materials" but are labeled by the FCC as comments.

The FCC Electronic Comments Filing System (ECFS) allows for search to include or exclude Express Comments, but it does not indicate that Express Comments timely filed during the period following a notice of proposed rulemaking will be treated differently from other comments. The FCC's welcome to the ECFS system states that it "serves as the repository for official records in the FCC's docketed proceedings from 1992 to the present."[86] That screen highlights proceedings with large numbers of comments filed, the first of which is the *Internet Freedom* docket. The screen allows visitors to click "Add New Filing or Express Reply," and when Express Reply is clicked the next page states "Note: You are filing a document into an

[82] Open Internet 2015 Decision, *supra* note 7, at ¶ 13, 80 FR 19738.
[83] Lauren Moxley, *E-Rulemaking and Democracy*, 68 ADMIN. L. REV. 661, 672 (2016).
[84] The White House, Executive Order 13579, Regulation and Independent Regualtory Agencies, July 11, 2011, https://obamawhitehouse.archives.gov/the-press-office/2011/07/11/executive-order-13579-regulation-and-independent-regulatory-agencies (last visited August 29, 2017).
[85] Moxley, *supra* note 83, 695.
[86] FCC, Welcome to the Electronic Comments Filing System, https://www.fcc.gov/ecfs/browse-popular-proceedings (last visited August 29, 2017).

official FCC proceeding. All information submitted, including names and addresses, will be publicly available via the web."[87] It does not state that Express Reply Comments will be excluded from the record or accorded any less weight than those submitted through the link "New Filing." The FCC cannot now changes its policy *sub silento* and wholesale discount comments filed through the Express Comment portal or ignore the allegations of identity theft and false filings being committed in the FCC proceeding through the FCC record and comment filing system.

Agency action based on "willful and unreasoning disregard of the facts and circumstances" constitutes arbitrary and capricious decision-making.[88] In *Office of Communication of United Church of Christ v. F.C.C.*, the D.C. Circuit commented that the "Commission and the Examiners have an affirmative duty to assist in the development of a meaningful record which can serve as the basis for the evaluation of the licensee's performance of his duty to serve the public interest. The Public Intervenors, who were performing a public service under a mandate of this court, were entitled to a more hospitable reception in the performance of that function."[89] Similarly, the FCC's duties to develop a meaningful record in a rulemaking proceeding and to treat the public hospitably and with respect are bedrock principles of law.

Code of Federal Regulations, 47 C.F.R. 1.1 confers onto the Commission the authority to "on its own motion or petition of any interested party hold such proceedings as it may deem necessary from time to time in connection with the investigation of any matter which it has power to investigate under the law, or for the purpose of obtaining information necessary or helpful in the determination of its policies, the carrying out of its duties or the formulation or amendment of its rules and regulations." The FCC abrogates its duties under federal law where it tolerates abuse of its process and criminal conduct in its proceeding while suggesting that it can deal with these issues merely by adjusting the weight of comments without investigation of these allegations. The FCC's apparent tolerance of criminal conduct in this proceeding demonstrates "willful and unreasoning disregard of the facts and circumstances," *Office of Communication of United Church of Christ v. F.C.C.*, 425 F.2d 543, 547, and arbitrary and capricious decision-making in violation of the APA.

The D.C. Circuit in *Prometheus Radio Broad. v. FCC*,[90] found that irregularities in the procedural conduct of an FCC rulemaking constituted arbitrary and capricious-decision making in violation of the APA. The FCC's tolerance of false filings based on identity theft fails the most basic tenants of fairness required by the APA. This rulemaking exceeds the procedural irregularities of *Prometheus* by countenancing criminal behavior in the comment process. The Commission's failure to address these concerns undermines the integrity of the FCC decision-making process and flunks the APA.

During my six year term when I served as a CPUC Commissioner, my colleagues and I voted to hold accountable and impose penalties on violators of CPUC rules requiring honesty,

[87] FCC, ECFS Express, https://www.fcc.gov/ecfs/filings/express (last visited August 29, 2017).
[88] *Probst v. State Dept. of Retirement Systems*, 167 Wash.App. 180, 192, n. 9 (Wash. Ct. App. 2012).
[89] *Office of Communication of United Church of Christ v. F.C.C.*, 425 F.2d 543, 547.
[90] 652 F.3d 431, 450 (3d Cir. 2011).

candor, and prohibiting misrepresentation in CPUC proceedings.[91] Under both state and federal law, integrity in the conduct of rulemakings is necessary to our system of government and a fundamental legal requirement. The FCC must investigate and take action to prevent criminal manipulation of its rulemaking process and hold accountable those responsible for false filings. Failure to do so abdicates the FCC's responsibilities.

Law enforcement and security agencies also must examine the connection between the bot filings, identity theft, and data breaches including the involvement of foreign actors such as Russians in the *Internet Freedom* proceeding. As discussed below, the FCC's proposal to allow ISPs to sell paid prioritization of Internet traffic would allow foreign entities and their agents to buy or bid up the price of U.S. Internet priority, restrained only in part by applicable sanctions. The FCC's proposal to allow paid Internet priority without constraining rules or FCC jurisdiction raises national security concerns. These proposals may be relevant to the motives for the bot swarm, identity theft, false filings, and foreign comments in the *Internet Freedom* proceeding.

III. Russian Comments in the *Internet Freedom* Rulemaking Raise National Security Concerns in light of Allegations of False Filings and a Bot Swarm

The FCC *Internet Freedom* docket contains 444,718 comments as of August 4, 2017 that purport to be filed by people residing in Russia as indicated by a search for the Cyrillic name Россия in the ECFS database.[92] All of the top ten filers with Россия in the text as listed by the FCC search use the same address "улица Полевая кв. 391 Челябинск, Россия." These comments state their support for maintaining net neutrality rules, but the number and similarity of comments submitted with the same Россия [Russia] address and reports of Russian hacking into U.S. databases call into question the motives and origin of those comments. The National Legal and Policy Center alleged on June 7, 2017 that express comments were filed from foreign email addresses including a Russian email address with a .Ru domain.[93] These comments purport to be the views of individuals listing one address in Russia. Authories must examine whether, in fact, these comments are part of a disinformation or influence campaign intended to provoke a reaction to Russian filings while one or more bot swarms and comments based on identity theft and data breaches advocate for repeal of FCC net neutrality rules.

---

[91] *See, e.g.*, CPUC, Decision 15-12-016, Decision Affirming Violations Of Rule 8.4 And Rule 1.1 And Imposing Sanctions On Southern California Edison (SCE) Company, December 3, 2015 (imposing a more than $16 million penalty on Southern California Edison for ten violations of the Commission's Rules and two violations of Rule 1.1, the Commission's Ethics Rule. The decision finds that the acts and omissions of SCE and its employees misled the Commission, showed disrespect for the Commission's Rules, and undermined public confidence in the agency.); CPUC Decision 15-04-024, Decision On Fines And Remedies To Be Imposed On Pacific Gas And Electric Company For Specific Violations In Connection With The Operation And Practices Of Its Natural Gas Transmission System Pipelines, April 9, 2015 (imposing $1.6 billion in fines and penalties and other remedies against Pacific Gas & Electric (PG&E) in the investigation of the natural gas pipeline explosion in San Bruno, California in 2010 for violations of CPUC rules including Rule 1.1 requiring candor and cooperation with the Commission, and for violations of other CPUC rules, orders, decisions, and the California Public Utilities Code).

[92] See FCC, ECFS, Express Comments, Yes, Search full text Россия (search conducted August 4, 2017), https://www.fcc.gov/ecfs/search/filings?express_comment=1&proceedings_name=17-108&q=%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F&sort=date_disseminated,DESC.

[93] Peter Flaherty, Analysis: *Fake Pro-Net Neutrality Public Comments Flood FCC From Russia, Other Foreign Countries*, National Legal and Policy Center, June 7, 2017, http://nlpc.org/2017/06/07/analysis-fake-pro-net-neutrality-public-comments-flood-fcc-russia-foreign-countries/.

Authorities must determine whether someone is "spoofing" those filings to make it appear that they are coming from Russia through a .Ru domain or physical address, while, in fact, they come from a different source. Use of a .Ru internet domain in a U.S. public filing or disclosing that the person commenting is located in Russia is not consistent with public reports of Russian tactics used to influence the U.S. elections by posing as a United States person in social media posts during the 2016 election season.[94]

Authorities must determine if someone is filing false statements that appear to come from abroad in order to influence the FCC decision-making process. "Disinformation campaigns" are one of the "active measures" the KGB has deployed to sow discord and wage information warfare."[95] Investigators must determine if these comments are part of a misdirection campaign perpetrated by foreign or U.S. persons or organizations while false filings based on identity theft urge repeal of the *2015 Open Internet Order* and a bot swarm afflicted the comment system.

Law enforcement should examine all of the allegations of false filings based on identity theft and allegations of fake comments using address generators in the *Internet Freedom* rulemaking to determine the source of these filings − whether foreign or domestic − and their motivation. The allegation of false filings through at least August 4 using an address generator and the FCC's ongoing display of allegedly false statements based on identity theft continue past President Trump's signing of the *Countering America's Adversaries Through Sanctions Act* on August 2, 2017. Authorities must investigate these activities to determine if they are part of a foreign influence operation or attempt to undermine the cybersecurity of the democratic decision-making process, and if they were conducted by sanctioned persons or entities.

The *Countering America's Adversaries Through Sanctions Act* imposes sanctions on any person who "knowingly engages in significant activities undermining cybersecurity against any person, including a democratic Institution, or government on behalf of the Russian federation."[96] Sanctioned "significant activities" that undermine cybersecurity are defined in that Act to include significant efforts to "exfiltrate, degrade, corrupt, destroy, or release information from such a system or network without authorization for purposes of—(i) conducting influence operations"[97] Data exfiltration is "the unauthorized copying, transfer or retrieval of data from a computer or

---

[94] *See, e.g.*, Massimo Calabresi, *Inside Russia's Social Media War on America*, TIME, May 18, 2017 ("In one case last year, senior intelligence officials tell TIME, a Russian soldier based in Ukraine successfully infiltrated a U.S. social media group by pretending to be a 42-year-old American housewife and weighing in on political debates with specially tailored messages."), http://www.google.com/amp/amp.timeinc.net/time/4783932/inside-russia-social-media-war-america/%3fsource=dam.

[95] Natasha Bertrand, *It looks like Russia hired internet trolls to pose as pro-Trump Americans*, BUSINESS INSIDER, July 27, 2016, http://google.com/amp/s/amp.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7.

[96] *Countering America's Adversaries Through Sanctions Act, supra* note 9, Title II (224) (a)(1)(A(Imposing an effective date for the imposition of sanctions on and after the date that is 60 days after the date of the enactment of this Act). While sanctions must be imposed within 60 days of August 2, 2017, the date of the Act's signing, the bill does not limit sanctions to activity that occurs on or after that date. The President of the United States is directed to impose sanctions under this Act "with respect to any person that the President determines (A) knowingly engages in significant activities undermining cybersecurity against any person, including a democratic institution, or government on behalf of the Government of the Russian Federation." The Act does not limit the timeframe for the activities that can form the basis for sanctions, only the date by which the imposition of sanctions must begin.

[97] *Id.* at Title II (A) 224(d)(1)(B)(i).

server."[98] Authorities must evaluate the comment process in this rulemaking to determine if individuals, entities, or governments violated the 2017 *Countering America's Adversaries Through Sanctions Act* or other laws. Investigation of false filings based on identity theft and the bot swarm must determine if foreign entities or agents, including those affiliated with Russia, North Korea, or other unfriendly nations, are responsible for those filings and the bot swarms. Those responsible parties must be held accountable for violations of U.S. laws including applicable sanctions.

This review must also consider the dangers to national security, democracy, the U.S. economy and polity posed by the FCC's proposal to allow unregulated paid Internet priority. The FCC proposes no rules or legal restrictions on the sale of Internet priority. This proposal would allow foreign governments, entities, or agents, as well as domestic sources, to create Internet bottlenecks and even blockades through unregulated paid prioritization.

IV. Paid Prioritization Proposals Raise National Security, Democratic Freedom, Economic, and Legal Enforcement Concerns

A. Unregulated Paid Prioritization Increases Risks to America's National Security and Democracy

Proposals to permit unregulated paid prioritization on the Internet reflect a September 11-type of failure of imagination about risks to America's national security and democracy. Foreign governments and their agents would relish the opportunity to buy priority Internet access to slow American messages or create a priority blockade. Paid prioritization may allow foreign governments or agents to gain a military advantage by manipulating U.S. Internet access and speeding their messages ahead. Foreign or domestic entities that buy or bid up the price for Internet priority could prop up an influence campaign or obtain the upper hand in economic competition such as time-constrained bidding.

The FCC's *Internet Freedom NPRM* fails to ask or analyze whether its proposals increase threats to national security or democracy. The FCC fails to connect the dots between the dangers of allowing any person or entity, including foreign actors or agents, to buy paid prioritization in an unregulated U.S. Internet market if the FCC adopts its proposal. This colossal omission recalls the failure of imagination that contributed to the September 11 attacks against our nation.[99] U.S. democracy, national security, public safety, military preparation, critical infrastructure, elections, education, innovation, and our national economy are increasingly dependent on the Open Internet that the FCC proposals put at risk.

The FCC's *Internet Freedom NPRM* seeks comment on the need for rules prohibiting paid prioritization for transmission of Internet data.[100] The FCC proposes no limits on who could buy paid prioritization, nor does the FCC propose any protections for Internet users against service or access degradation arising from paid prioritization of select users. The FCC's "lead

[98] Techopedia (July 29, 2017), https://www.techopedia.com/definition/14682/data-exfiltration.
[99] The 9/11 Commission Report, Final report of the National Commission on Terrorist Attacks upon the United States (2004), Ch. 11, Imagination, http://www.9-11commission.gov/report/911 Report.pdf.
[100] *Internet Freedom NPRM*, *supra* note 1, at ¶ 85.

proposal" to reclassify ISPs as "information service providers"[101] would remove the jurisdictional basis to respond to complaints about paid prioritization or to enforce the open Internet principles the FCC claims to espouse.[102] The FCC's proposal to eviscerate the jurisdictional basis for enforcement of Open Internet rules under Title II leaves our nation vulnerable to cyber blockades caused by paid prioritization.

Other bodies of law are inadequate to shield American Internet innovation from harm. U.S. sanctions against foreign governments, individuals, or entities provide only limited protections against transactions that may compromise America. Cybersecurity sanctions against Russia restrain only those working on behalf of the government of the Russian federation.[103] The *Countering America's Adversaries Through Sanctions Act* imposes penalties on any person who "knowingly engages in significant activities undermining cybersecurity against any person, including a democratic Institution, or government on behalf of the Russian federation."[104] The limited applicability of cybersecurity sanctions to those working "on behalf of the Government of the Russian Federation" creates incentives to profess no Russian governmental involvement in activities that would otherwise be subject to sanction. Subterfuge and even hijacking of American phones, computers, and connected devices could also be deployed to attempt to evade American sanctions.

If permitted to sell paid Internet prioritization in the United States, ISPs would be challenged to identify whether they are selling Internet priority to sanctioned persons or entities. Amazon is cooperating with the U.S. Treasury on investigations of sales of goods ranging from software to pet food to individuals with ties to the Iranian government, as well as to an Iranian embassy. [105] Treasury is examining whether these sales violated the Iran Threat Reduction and Syria Human Rights Act of 2012, and the U.S. has brought charges against individuals in China accused of acting as shell companies to evade sanctions against North Korea.[106] ISPs could believe in good faith they are selling U.S. Internet priority to persons or entities not subject to sanctions. An ISP would face investigation and potential penalties if the buyer or the buyer's benefactor turns out to be a sanctioned individual or organization. Some people or organizations, whether domestic or foreign, may seek to buy or hack paid prioritization for nefarious, even criminal purposes. National security would be compromised if unregulated paid prioritization delays or blocks U.S. messages during times of congestion, emergency, or critical activity such as elections or natural disasters.

---

[101] *Id.* at ¶ 100.
[102] *Id.* at ¶ 70 ("Proposing to restore broadband Internet access service to its long-established classification as an information service reflects our commitment to a free and open Internet.")
[103] *Countering America's Adversaries Through Sanctions Act*, *supra* note 9, 224(a)(1)(A).
[104] *Id.*
[105] Jill Disis, *Amazon Says it Might Have Violates U.S. Sanctions on Iran*, CNN MONEY, August 1, 2017, http://money.cnn.com/2017/08/01/news/companies/amazon-iran-sanctions-investigation/index.html; Ari Shapiro, *Shell Companies Enable to Dodge Economic Impact of Sanctions*, NPR, August 7, 2017 (broadcasting interview with Anthony Ruggiero of the Foundation for Defense of Democracies about how North Korean shell companies enable the country to circumvent the economic impact of sanctions), http://www.npr.org/2017/08/07/542086977/shell-companies-enable-north-korea-to-dodge-economic-impact-of-sanctions; Michael Forsythe, *U.S. Says Chinese Executive Helped Dodge North Korea Sanctions*, NEW YORK TIMES, September 27, 2016, https://www.nytimes.com/2016/09/28/world/asia/china-north-korea-sanctions-ma-xiaohong.html.
[106] *Id.*

The FCC's *Internet Freedom NPRM* contemplates paid prioritization at the individual user level asking: "Could allowing paid prioritization enable certain critical information, such as consumers' health care vital signs that are being monitored remotely, to be transmitted more efficiently or reliably?"[107] This question contemplates paid Internet priority for an individual user's data, a proposal that could create both localized and network risks.

Comcast's comments urged "a more flexible approach to prioritization" citing the example that "a telepresence service tailored for the hearing impaired requires high-definition video that is of sufficiently reliable quality to permit users "to perceive subtle hand and finger motions" in real time."[108] AT&T's comments argue that paid prioritization "of packets traversing multiple IP networks—is unlikely to become a commercial reality anytime soon, and there is no valid basis for a categorical ban on this theoretical practice that can be expected to benefit consumers if and when it is implemented."[109]

Paid prioritization would not have to traverse multiple IP networks to raise concerns for others sharing the same Internet network, particularly if priority were localized. AT&T argues against the *2015 Open Internet Order* ban on paid prioritization stating "[s]uppose, for example, that ISPs began implementing isolated paid-prioritization arrangements to support quality of service ("QoS") for unusually latency-sensitive applications, such as high-definition videoconferencing or massively multiplayer online gaming ("MMOG")."[110] This example presupposes an "isolated paid-prioritization arrangement" to support videoconferencing or gaming. The FCC's *Internet Freedom NPRM* does not require that paid prioritization be isolated from or not diminish the service of other Internet users.

The FCC's proposal would leave Americans needing remote health monitoring, as well as the American government, military, business, and all Americans, at risk of being outbid by others for Internet priority. Without safeguards to ensure that other Internet users are not harmed by prioritization, the FCC's proposal may allow ISPs to "deprioritize" the signals of other Americans to speed ahead those who pay for Internet priority.

The FCC's proposal would permit ISPs to ask or to allow individual Twitter users, for example, to pay for priority or risk being outbid by others that buy priority first or pay more. The FCC's *Internet Freedom NPRM* envisions Internet priority sold at the local level. This proposal could affect Internet access in American neighborhoods ranging from the White House area to Midwestern towns, financial districts, residential neighborhoods, port cities, rural, urban, and suburban areas. Government agencies, critical infrastructure, health care providers and patients, students and educational institutions, businesses, and the American military including defense contractors could face the choice of paying extra for priority Internet access or waiting behind or even being blocked by those with paid priority.

---

[107] *Internet Freedom NPRM*, *supra* note 1, at ¶ 93.
[108] Comments of Comcast Corporation, *In the Matter of Restoring Internet Freedom*, 17-208, at 56 (July 17, 2017), https://ecfsapi.fcc.gov/file/107171777114654/2017-07-17%20AS-FILED%20Comcast%202017%20Open%20Internet%20Comments%20and%20Appendices.pdf.
[109] Comments of AT&T Services Inc., *In the Matter of Restoring Internet Freedom*, 17-208, at 5 (July 17, 2017), https://ecfsapi.fcc.gov/file/10717906301564/AT%26T%20Internet%20Freedom%20Comments.pdf.
[110] *Id.* at 36.

The March 2017 report of Russian attempts to place malware on Twitter accounts of U.S. Defense Department employees reveals risks of the paid prioritization proposal.[111] TIME Magazine reported that U.S. counterintelligence officials learned that Russians "sent expertly tailored messages carrying malware to more than 10,000 Twitter users in the Defense Department…offer[ing] links to stories on recent sporting events or the Oscars."[112] "When clicked, the links took users to a Russian-controlled server that downloaded a program allowing Moscow's hackers to take control of the victim's phone or computer-and Twitter account."[113] "Now counterintelligence officials wondered: What chaos could Moscow unleash with thousands of Twitter handles that spoke in real time with the authority of the armed forces of the United States?"[114] "At any given moment, perhaps during a natural disaster or a terrorist attack, Pentagon Twitter accounts might send out false information."[115] "As each tweet corroborated another, and covert Russian agents amplified the messages even further afield, the result could be panic and confusion,"[116] TIME reported.

Through malware hackers can convert phones, computers, and things into hacker-controlled "bots," short for robots. The U.S. Computer Emergency Readiness Team, U.S. Cert, issued an alert in October 2016 warning that "IoT [Internet of things"] devices have been used to create large-scale botnets—networks of devices infected with self-propagating malware—that can execute crippling distributed denial-of-service (DDoS) attacks."[117] CERT warned "IoT devices are particularly susceptible to malware, so protecting these devices and connected hardware is critical to protect systems and networks."[118]

Cisco defines a malicious bot as "self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s)."[119] Bots can self-propagate, "log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DoS [Denial of Service] attacks, relay spam, and open back doors on the infected host."[120] Malicious bots can make computers including smart phones into "zombies" that recruit other computers to "act in unison, carrying out commands sent by the bot net owner.

---

[111] Calabresi, *supra* note 94.
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] U.S. Cert, (Alert TA 16-288A), *Heightened DDOS Threated Posed by Mirai and other Botnets*, Oct. 14, 2016, (defining the "Internet of Things (IoT)—an emerging network of devices (e.g., printers, routers, video cameras, smart TVs) that connect to one another via the Internet, often automatically sending and receiving data" and warning of vulnerability to hacking by botnets that commander the IOT resource to send Internet traffic including DDOS attacks), https://www.us-cert.gov/ncas/alerts/TA16-288A.
[118] *Id.*
[119] Cisco, *What's the Difference between Viruses, Worms, Trojans, and Bots*, http://www.cisco.com/c/en/us/about/security-center/virus-differences.html#6 (last visited August 2, 2017).
[120] *Id.*

These infections can be difficult to detect and eradicate."[121] In 2016 the malware known as Mirai scanned the Internet for insecure connected devices such as wireless routers and public video cameras, hacked device passwords, subjected the device to the command and control of a master computer, and used the hacked device to launch a Distributed Denial of Service attack at other targets.[122]

"Cybercriminals may also lease their botnets to other criminals who want to send spam, scams, phishing, steal identities, and attack legitimate websites, and networks."[123] The Washington Post reported that the National Security Agency found that the WannaCry virus unleashed in mid-May 2017 was a "computer worm to be paired with ransomware, which encrypts data on victims' computers and demands a ransom to restore access."[124] "WannaCry was apparently an attempt to raise revenue for the regime, but analysts said the effort was flawed. Though the hackers raised $140,000 in bitcoin, a form of digital currency, so far they have not cashed it in, the analysts said. That is likely because an operational error has made the transactions easy to track, including by law enforcement."[125] The Oxford Internet Institute documented the use of bots by dozens of government and military organizations for social media campaigns.[126]

These incidents indicate that hackers may seek to commandeer accounts that have paid prioritization and use them for nefarious activities. Bot masters could direct hacked accounts to obtain paid Internet priority. Hacked accounts that already subscribe to paid Internet priority could be harnessed to fortify a botnet Internet wall that creates roadblocks for other users without priority.

President Trump's Executive Order on Cybersecurity directed the Secretary of Commerce and the Secretary of Homeland Security to "jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)."[127] President Trump's Executive Order recognizes the danger of botnets to U.S. security. The FCC

---

[121] Andy O'Donnell, *5 Types of Malicious Bots and How to Avoid Them*, LIFEWIRE, July 30, 2017, https://www.lifewire.com/what-are-malicious-bots-2487156.

[122] Search Security, *supra* note 39.

[123] Webroot, What are Bots, Botnets, and Zombies, https://www.webroot.com/us/en/home/resources/tips/pc-security/security-what-are-bots-botnets-and-zombies.

[124] Ellen Nakashima, *The NSA has linked the WannaCry Computer Worm to North Korea*, THE WASHINGTON POST, June 14, 2017, https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.577aaebf24f2.

[125] *Id.*

[126] Bradshaw and Howard, *supra* note 51, at 4 (analyzing "cyber troops" in 25 countries, and defining cyber troops as "government, military or political party teams committed to manipulating public opinion over social media." Reporting that "cyber troops will often apply traditional offensive cyber tactics, such as hacking or surveillance, to target users for trolling or harassment campaigns…. An important distinction between cyber troops and other state-based actors operating in cyberspace is their role in actively shaping public opinion.")

[127] Exec. Order No. 13800, 82 FR 22391 § 2(d) (2017), Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, [hereinafter *Executive Order on Cybersecurity*], https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

must recognize the vulnerability of paid prioritization to hackers, a hazard compounded by the FCC's proposal to remove the jurisdictional classification that safeguards the Internet's open nature.

Paid Internet prioritization that delays, degrades, or impedes other Internet traffic, could increase create or exacerbate a local, regional, state, or national emergency. If a priority blockade or disruption were created by those subject to sanctions, *post-facto* penalties would apply to the parties to the banned transaction. Sanctioned "significant activities" include significant efforts to "deny access to or degrade, disrupt, or destroy an information and communications technology system or network."[128] Degradation, delay, or disruption of U.S. Internet traffic due to paid prioritization appears to fall within sanctioned conduct. Sanctions may not, however, be sufficient or timely to deter launch of an Internet priority blockade.

The FCC's *2015 Open Internet Order's* ban on paid prioritization underscored that "allowing for the purchase of priority treatment can lead to degraded performance—in the form of higher latency, increased risk of packet loss, or, in aggregate, lower bandwidth—for traffic that is not covered by such an arrangement."[129] As mentioned by the FCC's *Internet Freedom NPRM* the FCC's *2015 Open Internet Order* determined that "fast lanes" or "paid prioritization" practices "harm consumers, competition, and innovation, as well as create disincentives to promote broadband deployment."[130]

The *Internet Freedom NPRM* asks "could allowing paid prioritization give Internet service providers a supplemental revenue stream that would enable them to offer lower-priced broadband Internet access service to end-users?"[131] The *Internet Freedom NPRM* proposes no requirements for ISPs to channel revenues from paid prioritization into network improvements, broadband expansion, or lower prices. Paid prioritization may create disincentives to invest in facilities and services for all users and instead drive ISP profits or steer resources toward those who pay for fast-lane service. Paid prioritization without FCC oversight allows ISPs to earn revenue from network congestion. In 2013, Verizon lawyers argued in the D.C. Circuit Court of Appeals that the FCC's then-existing prohibitions on Internet blocking, throttling, and paid prioritization were "foreclosing potential revenue streams."[132]

ISP "deprioritization" of certain users with "unlimited Internet" plans foreshadow the slow to non-functional service non-prioritized users may face waiting behind the cordon of those with priority. The FCC fined AT&T $100 million in 2014 for inadequate disclosure to

---

[128] *Id.* at 224(d)(1)(A).

[129] *Open Internet 2015 Order*, 30 F.C.C. Rcd. 5601, 5654, n. 287 ("*See* Mozilla Comments at 20 ("Prioritization is inherently a zero-sum practice, and inherently creates fast and slow lanes and prevents a level playing field."); Mozilla Reply at 15; Sandvine Comments at 9 ("At a moment in time, there is a fixed amount of bandwidth available to all applications, content, etc. on a given network. If one application has paid for more of that bandwidth (and this is how the priority is achieved) then there is less 'best efforts' bandwidth remaining for all other applications and content."). *But see* ADTRAN Reply at ii, 6, 16 (arguing that the zero-sum game theory is incorrect because it ignores the fact that broadband providers' capacity is not static); Letter from Justin (Gus) Hurwitz, Assistant Professor, University of Nebraska College of Law, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 14-28, at 1 (filed Nov. 3, 2014) (asserting that prioritization is not "zero sum")).

[130] *Id.* at ¶ 85 (citing 47 C.F.R. 8.9; *2015 Open Internet Order*, 30 F.C.C. Rcd. 5601, ¶ 125).

[131] *Internet Freedom NPRM, supra* note 1, at ¶ 86.

[132] *Verizon v. FCC*, 740 F.3d 623, 649.

"unlimited plan" customers that their Internet speeds would be dramatically slowed if they used more than an undisclosed amount of data.[133] AT&T reduced deprioritized customer speeds to "256 kbps or 512 kbps" [kilobits per second," for an average of 12 days per billing cycle."[134] The FCC found those speeds "significantly impaired the ability of AT&T's customers to use their data service."[135] "Although a customer may be able to send an email at these speeds, he or she may find it impossible to use AT&T's data service in ways that most people today use smartphones—for instance, using mapping applications to get from one place to the next, streaming online video to catch up on television or news, or using video chat applications to stay connected with friends and family."[136] "A minimum download speed of approximately 700 kbps is necessary to use FaceTime or another video calling application, and 3.5 Mbps [megabits per second] is necessary to watch standard-definition television"[137] The FCC brought this enforcement action under the *2010 Open Internet Order* transparency rules which *Verizon v. FCC* upheld.[138]

In 2016 the FCC penalized T-Mobile $48 million for violations of 2015 Open Internet transparency rules for slowing customers in the top 3% of data users during times of congestion.[139] "Under its "Top 3 Percent Policy," T-Mobile "de-prioritizes" its "heavy" data users during times of network contention or congestion to speeds far below those advertised for the "unlimited" data plan."[140] Consumers reported to the FCC that "this policy rendered data services "unusable" for many hours each day and substantially limited their access to data."[141]

FCC rules under the *2010* and *2015 Open Internet Orders* allow "specialized services" such as "facilities-based VoIP offerings, heart monitors, or energy consumption sensors [which]—may be offered by a broadband provider but do not provide access to the Internet generally."[142] The FCC explained that the "term "specialized services" can be confusing because the critical point is not whether the services are "specialized;" it is that they are not broadband Internet access service."[143] In the *2015 Open Internet Order* the FCC required disclosure of "what specialized services, if any, are offered to end users, and whether and how any specialized services may affect the last-mile capacity available for, and the performance, or broadband Internet access service")."[144]

AT&T offers specialized services such as the ability of qualified emergency service providers to buy through a U.S. Homeland Security Application limited prioritization for their

---

[133] *In the Matter of AT&T Mobility, LLC.*, 30 F.C.C. Rcd. 6613 (2015).
[134] *Id.* at 6616.
[135] *Id.*
[136] *Id.*
[137] *Id.*
[138] *Id.* at 6613 (noting that "The 2015 Order became effective on June 12, 2015; the enhancements to the Transparency Rule are not in effect as of the date of this action.")
[139] *FCC Reaches $48 Million Settlement with T-Mobile to Address Inadequate Disclosures of Unlimited Data Plan Restrictions* , 2016 WL 6126190, at *1 (Oct. 19, 2016).
[140] *Id.*
[141] *Id.*
[142] *2015 Open Internet Order*, *supra* note 7, at ¶ 35.
[143] *Id.*
[144] *Id.* at ¶ 167.

urgent communications "not originating from or traversing the Internet."[145] Qualified Enterprise users who signed up for a special plan can mark up to "10 gigabytes (GB) of use per billing cycle" for Quality of Service treatment on a "differentiated" network.[146] These "specialized services" limit the buyers, quantity, and source of communication subject to priority, and ensure it does not degrade service for other users sharing the same last-mile capacity.

AT&T has obtained the contract to create First Net, which is being constructed to provide a communications channel for first responders. The FCC's proposal to allow for paid prioritization is not necessary to support emergency service provider Internet communications. Indeed, it may harm emergency service providers and agencies coordinating to handle disasters that do not or are not entitled to use First Net as it would subject them to delays or failures due to other users with paid priority.

The FCC's "general conduct" rule also constrains "specialized services" to prevent ISP action contrary to the 2015 Open Internet rules and principles. The FCC *Internet Freedom NPRM* proposes to eliminate the "general conduct" standard adopted in the 2015 *Open Internet Order*,[147] as well as the jurisdictional basis to safeguard against Internet degradation from paid prioritization including diminished service for emergency personnel.

The Body of European Regulators (BERC) issued guidelines in August 2016 to protect the open Internet while allowing for "specialised services" such as remote surgery.[148] BERC guidelines require that such "specialised services" not degrade the experience of other Internet Access Service (IAS).[149] "Specialised services" in the European Community are subject to the

---

[145] *See, e.g.*, specialized services consistent with the *2015 Open Internet Order*, AT&T, Wireless Priority (providing priority for calls from Emergency Agencies available through an application from the U.S. Homeland Security site), https://www.wireless.att.com/businesscenter/business-programs/government/wireless-priority.jsp; AT&T, AT&T Dynamic Traffic Management − Public Safety (allowing public safety agencies to "prioritize their mission-critical data traffic on the AT&T- owned domestic 4G LTE network," a service "available only to qualified local, state and federal emergency management organizations (such as police and fire departments). The service is not available for unlimited plans and "does not apply to your [public safety agency] data traffic originated on or traversing over the Internet"), https://www.corp.att.com/stateandlocal/docs/ADTM-Public_Safety.pdf.

[146] AT&T, AT&T Dynamic Traffic Management − Enterprise (enabling "qualified enterprise and government customers to receive priority treatment (not priority access) on the AT&T-owned domestic 4G LTE network for approved business applications. By segregating data traffic using QoS, enterprise customers can prevent non-critical apps from impeding business critical apps." Offered as "an enhancement to authorized Corporate Responsible User (CRU) lines of service." "Each CRU line requires (a) a qualified data plan with a specific data allowance (no unlimited plans) and (b) a 4G LTE-compatible device provisioned with an Approved Business Application." "Authorized CRUs using AT&T Dynamic Traffic Management – Enterprise are limited to 10 gigabytes (GB) of use per billing cycle; any data traffic sent by an authorized CRU after the 10 GB allotment will be handled on "best effort" QoS.), https://www.business.att.com/content/productbrochures/dynamic-traffic-management-product-brief-enterprise.pdf.

[147] *Internet Freedom NPRM*, *supra* note 1, at ¶ 49.

[148] Body of European Regulators (BERC), BEREC GUIDELINES ON THE IMPLEMENTATION BY NATIONAL REGULATORS OF EUROPEAN NET NEUTRALITY RULES, ARTICLE 3.5, SEC. 102 (Aug. 2016) (requiring that "specialised services are not to the detriment of the availability or general quality of the IAS [Internet Access Services] for end-users"), http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules.

[149] *Id.*

condition that "network capacity is sufficient to provide the specialised service in addition to any IAS provided; specialised services are not usable or offered as a replacement for IAS; specialised services are not to the detriment of the availability or general quality of the IAS for end-users."[150]

The FCC's *Internet Freedom NPRM* offers no shield for Internet users without priority, and no jurisdictional basis upon which to respond to complaints or threats to Internet openness. Neither can ISPs be counted on to safeguard Internet openness and protect users who do not pay for priority as paid prioritization skews their incentive to protecting that revenue source. ISP contract terms provide no safe harbor for consumers as ISPs do not incorporate policies not to block or throttle Internet users into their contracts and reserve a right to modify their contracts at any time. ISPs may be focused on the opportunity for paid prioritization to enhance their revenues or create new service. Yet, the FCC must not be blinded by the failure to imagine the ways in which paid priority could be manipulated or hijacked so it causes congestion, degrades other Internet users, and erects cyber-barricades. ISP self-regulation, antitrust, and unfair competition laws are insufficient to address these threats and offer no remedy for harms to democracy or national security.

B. ISP "Self-Regulation," Contract, Antitrust and Consumer Protection Laws Cannot Substitute for Enforceable FCC Jurisdiction to Protect Internet Openness and Respond to Complaints

The *Internet Freedom NPRM* asks: "What are the trade-offs in banning business models dependent on paid prioritization versus allowing them to occur when overseen by a regulator or industry actors?[151] "To the extent we decide to retain any of the Commission's *ex ante* regulations," the NPRM queries, "we seek comment on whether, and how, we should modify them, specifically considering different approaches such as self-governance or *ex post* enforcement that may effectuate our goals better than across-the-board rules."[152] The FCC does not discuss any legal theory by which it could retain its jurisdiction as a regulator to enforce rules against diminished or even blocked service to accommodate paid priority if its adopts its lead proposal to drop the classification of ISPs under Title II.

ISP "self-governance" through their contract terms cannot be relied upon by the FCC, the public, or ISP consumers to protect Internet Openness or limit ISP blocking, throttling, or paid prioritization. As discussed in my Op Ed, *Protect the Open Internet*, attached as Exhibit C, "[m]any major ISPs post policy statements on their web sites proclaiming that the ISP does not block or throttle data, but these policies are excluded from their consumer contracts."[153] "These statements are neither written in the language of promise nor condition, nor are they integrated into user agreements, rendering them unenforceable in contract."[154] Even if ISPs incorporated into their contract a promise not to block, throttle, or engage in paid prioritization, "most ISPs

[150] *Id.* at Sec. 102.
[151] *Internet Freedom NPRM*, *supra* note 1, at ¶ 85.
[152] *Id.* at ¶ 70.
[153] Catherine J.K. Sandoval, *Protect the Open Internet*, DAILY JOURNAL, May 19, 2017.
[154] *Id.*

reserve the right to modify their Internet Service contract at their discretion and contend that continued use of the service constitutes agreement."[155]

My Reply Comments in the FCC's 2010 Open Internet proceeding analyzed in detail the restrictive terms in many ISP contracts that limited the use of certain types of Internet protocols or content.[156] My analysis revealed that in 2010 "many wireless ISP TOS [Terms of Service] and AUP [Acceptable Use Policy] documents prohibit the use of Internet protocols such as Peer-to-Peer (P2P) or Voice Over Internet Protocol (VoIP), or proscribe downloading or uploading certain types of content such as movies or games."[157]

The FCC 2017 *Internet Freedom NPRM* asks whether bright line or *ex ante* rules are needed to prohibit discrimination or protect the open Internet. The FCC inquires, "[b]eyond the few, scattered anecdotes cited by the *Title II Order*, have there been additional, concrete incidents that threaten the four Internet Freedoms sufficient to warrant adopting across-the-board rules?"[158] This question ignores the evidence I submitted in my 2010 Reply Comments documenting widespread discrimination against certain protocols such as P2P, VoIP, and proscriptions against certain types of content such as movies or games, all restricted by ISP contracts in their terms of use policy.[159] The FCC discussed my comments in its 2010 decision, emphasizing that "broadband providers' terms of service commonly reserve to the provider sweeping rights to block, degrade, or favor traffic."[160] The FCC's 2010 *Open Internet Order* cited as examples of the need for enforceable Open Internet rules that "one major cable provider reserves the right to engage, "without limitation," in "port blocking, . . . traffic prioritization and protocol filtering."[161] The FCC noted that "a major mobile broadband provider prohibits use of its wireless service for "downloading movies using peer-to-peer file sharing services" and VoIP applications."[162]

My 2014 comments submitted in the 2015 *Open Internet* proceeding highlighted my 2010 comments that "analyzed wireless and cable ISP contracts, terms of use, and exclusions, and concluded that many representations in those documents were inconsistent with the unbridled, even "unlimited" Internet access many ISPs promised subscribers."[163] The FCC's *2014 NPRM* in the *Open Internet* rulemaking highlights "consumer reports of "surprise at broadband providers' statements about slowed or terminated service based on consumers' "excessive use."[164]

---

[155] *Id*.
[156] *Professor Sandoval 2010 Preserving the Open Internet Reply Comments, supra* note 7.
[157] *Id*. at 4.
[158] *Internet Freedom NPRM, supra* note 1, at ¶ 77.
[159] *Professor Sandoval 2010 Preserving the Open Internet Reply Comments, supra* note 7, at 4.
[160] *2010 Open Internet Order, supra* note 7, at 17926 (citing Sandoval reply [*Professor Sandoval 2010 Preserving the Open Internet Reply Comments, supra* note 7], 43-54).
[161] *Id*. (citing WCB Letter 12/10/10, Attach. at 81-92, Cox Communications, Cox High-Speed Internet Acceptable Use Policy, ww2.cox.com/aboutus/policies.cox).
[162] *Id*. (citing WCB Letter 12/10/10, Attach. at 30-34, MetroPCS, MetroWEB Terms of Use, www.metropcs.com/products/metroweb/terms_of_use.aspx).
[163] *Commissioner Sandoval 2015 Open Internet Ex Parte Comments, supra* note 7, at 67.
[164] *Id*. at 67-68 (citing *In the Matter of Protecting & Promoting the Open Internet*, NPRM, 29 F.C.C. Rcd. 5561, 5587 (GN Docket No. 14-28) (2014) [hereinafter *Open Internet 2014 NPRM*] ("Consumers have also reported

Carrier inclusion of contract terms prohibiting but not defining "excessive use" is explored in my 2009 Article, *Disclosure, Deception, and Deep Packet Inspection, The Role of the Federal Trade Commission Act in the Net Neutrality Debate*."[165] My 2014 comments emphasized that "[c]onsumer complaints to the FCC underscore how some carriers use broad reservations in posted contract terms to limit Internet access advertised as wide-ranging or unlimited, or to terminate subscribers."[166] ISP contractual terms that prohibit particular protocols or types of uses deter consumers, innovators, and investors in those protocols or services.[167]

Most ISPs reserve the right to use arbitration to resolve consumer complaints. ISP records would show how often they exercised these contractual limitations to charge consumers more or terminate their contracts. The FCC's *2014 NPRM* that led to the *2015 Open Internet Order* highlights "consumer reports of "surprise at broadband providers' statements about slowed or terminated service based on consumers' 'excessive use'."[168] Those complaints to the FCC are evidence of ISPs' using contractual terms to charge consumers more or terminate their contracts. These ISP contract terms provide evidence of concrete harms that supported the FCC's *2015 Open Internet Order*. ISP enforcement of those terms through overcharges, consumer termination, or in arbitration rests provides more evidence of concrete harms when no enforceable Open Internet rules were in place. The *Internet Freedom NPRM*'s characterization of harms to Internet openness as only demonstrated by "a few scattered anecdotes"[169] ignores this record, demonstrating arbitrary and capricious decision-making in violation of the APA.

This proceeding must also analyze the change in ISP terms of service after the 2015 Open Internet Order to provide contract terms consistent with that order. My analysis of the 2017 terms of service and acceptable use policies for major ISPs AT&T, Verizon, and Comcast shows no current restrictions on particular protocols such as Peer-to-Peer, and nor restrictions on types

---

surprise at broadband providers' statements about slowed or terminated service based on consumers' "excessive use." Other consumers report confusion about how data consumption is calculated for purposes of data caps.")

[165] Catherine J. K. Sandoval, *Disclosure, Deception, and Deep-Packet Inspection: The Role of the Federal Trade Commission Act's Deceptive Conduct Prohibitions in the Net Neutrality Debate*, 78 FORDHAM L. REV. 641, 681 (2009) [hereinafter Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*].

[166] *Id*.

[167] *Cf.* Opening Comments of Vimeo Inc., (WC Docket No. 17-108), at 5, 9 ("Vimeo provides consumers with tools to upload, share, and watch original videos."…"If broadband providers could block, throttle, or charge arbitrary fees, Vimeo's incentive to make capital investments would be severely reduced."), https://ecfsapi.fcc.gov/file/10717185758722/2017%20NPRM%20Vimeo%20Opening%20Comments%207-17-17%20FINAL.pdf.

[168] *Commissioner Sandoval 2015 Open Internet Ex Parte Comments*, *supra* note 7, at 67-68 (citing *Open Internet 2014 NPRM*, 29 F.C.C. Rcd. 5561, 5587).

[169] *Internet Freedom NPRM*, *supra* note 1, at ¶ 77.

of uses such as the downloading of movies, video, or use of VoIP.[170] This is a major shift since my 2010 analysis of ISP contract terms submitted in the record for the 2010 Open Internet proceeding,[171] which found a widespread practice of ISP reservation of rights to proscribe certain protocols or uses.[172] The *2015 Open Internet Order* made restrictions on particular protocols a violation of that decision, and limited ISPs to reasonable network management.[173] While some ISPs today use "dynamic congestion management" techniques that slow heavy users during congestion, none of the three ISPs studied, Comcast, AT&T, or Verizon, prohibited a particular protocol or type of use such as video.[174]

The *Internet Freedom NPRM* asks "[i]s there any evidence that the likelihood of these events occurring decreased with the shift to Title II?"[175] The shift in ISP terms of service and acceptable use policies to eliminate their reservation of right to block or throttle particular protocols or types of uses such as video, games, or VoIP, demonstrates that the *2015 Open Internet Order* reduced the likelihood of such discrimination occurring because it made doing so a violation of FCC rules. The prevalence of ISP contract terms that limit particular protocols or

[170] *See, e.g.*, Xfinity, Residential Service Agreement, (Comcast provides its customers with full access to all the lawful content, services, and applications that the Internet has to offer. Comcast does not block or rate-control specific protocols or protocol ports (except to prevent spam, malicious attacks, and identity theft), does not modify protocol fields in ways not prescribed by protocol standards, and does not otherwise inhibit or favor certain applications or classes of applications), https://www.xfinity.com/Corporate/Customers/Policies/SubscriberAgreement.html; Xfinity, Network Management Information, (congestion-managed traffic is not based on specific applications or content, but on current network conditions and recent amounts of data transferred by users), https://www.xfinity.com/support/internet/network-management-information/; AT&T Acceptable Use Policy, (AT&T prohibits use of the IP Services in any way that is unlawful, harmful to or interferes with use of AT&T's network or systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, infringes intellectual property rights, results in the publication of threatening or offensive material, or constitutes Spam/E-mail/Usenet abuse, a security risk or a violation of privacy), https://www.att.com/legal/terms.openinternetpolicy.html; Verizon, Verizon Open Internet Policy, ("On any of our Internet access services, wireline or wireless, you and other users of our service can access and use the legal content, applications, and services of your choice, regardless of their source.), http://www.verizon.com/about/sites/default/files/Verizon_Broadband_Commitment.pdf.; Verizon, Online Terms of Service, http://www.verizon.com/about/sites/default/files/Internet-ToS-04142017-v17-2-ENGLISH.pdf.

[171] *Professor Sandoval 2010 Preserving the Open Internet Reply Comments*, *supra* note 7.

[172] *Internet Freedom NPRM*, *supra* note 1, at ¶ 13, n. 36 (citing Michael K. Powell, Chairman, Federal Communications Commission, Preserving Internet Freedom: Guiding Principles for the Industry, Remarks at the Silicon Flatirons Symposium (Feb. 8, 2004) (announcing Internet Freedom principles including "the freedom to access lawful content, the freedom to use applications, the freedom to attach personal devices to the network, and the freedom to obtain service plan information"), https://apps.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf.

[173] *2015 Open Internet Order*, 30 F.C.C. Rcd. 5601, at Appendix A, ¶¶14, 32.

[174] Xfinity, Learn How Network Congestion Management Affects Your Internet Use, ("Our technique does **not** manage congestion based on specific online activities, protocols or applications that a customer uses. Rather, it only focuses on the heaviest users in real time, so that congestion periods tend to be fleeting and sporadic. It is important to note that the effect of this technique is temporary and has nothing to do with a customer's aggregate monthly data usage. Rather, it's dynamic and based on prevailing network conditions as well as a customer's data usage over a very recent period of time.")(emphasis in the original), https://www.xfinity.com/support/internet/network-management-information/.

[175] *Internet Freedom NPRM*, *supra* note 1, at 50.

types of uses prior to legally enforceable Open Internet rules is evidence of "concrete incidents that threaten Internet Freedoms and warrant enforceable rules to prevent their exercise."[176]

This change in terms of service was driven by the shift in FCC regulations, not a market-driven swing. When the FCC did not explicitly prohibit discrimination against particular protocols or types of uses, many carriers limited those protocols through their contract terms as discussed extensively in my 2010 Open Internet comments, my 2015 Open Internet comments, and my article *Disclosure, Deception, and Deep Packet Inspection, The Role of the Federal Trade Commission Act in the Net Neutrality Debate*."[177] FCC regulation made the difference and removal of that regulation will open the legal door to new restrictions by ISPs who act as gatekeepers to the Internet.

Consumer complaints to the FCC underscore how some carriers use broad reservations in posted contract terms to limit Internet access. The FCC's 2014 *Open Internet NPRM* cited evidence of customer surprise when they were terminated or cut off for violating those or other rules limiting use of their "unlimited" service.[178] The FCC's 2015 $100 million fine against AT&T and the 2016 $48 million fine against T-Mobile for dramatically throttling customers who had "unlimited plans" when their use exceeded an undisclosed threshold provide more evidence of concrete incidents that threaten Internet freedoms and warrant enforceable rules.[179]

Instead of discussing the enforcement record for the 2010 or *2015 Open Internet Order's* transparency rules or orders, the *Internet Freedom NPRM* questioned the need for enforceable rules to restrain ISP behavior. The *NPRM* claimed "[m]uch of the *Title II Order* focused extensively on hypothetical actions Internet service providers "might" take, and how those actions "might" harm consumers, but the *Title II Order* only articulated four examples of actions Internet service providers arguably took to justify its adoption of the Internet conduct standard under Title II.[180] The FCC asked "[i]s there evidence of actual harm to consumers sufficient to support maintaining the Title II telecommunications service classification for broadband Internet access service?[181]

The National Hispanic Media Coalition (NHMC) in May 2017 filed a Freedom of Information Act Request asking for records of "47,000 open Internet complaints that it [the FCC] has received." [182] The FCC on July 17, 2017 denied NHMC's request for an extension of time to file comments in the *Internet Freedom* docket in light of the FCC's failure to fully comply with this records request.[183] The Voices Coalition which includes NHMC reported in their *Internet Freedom* comments that during a follow-up phone conversation on June 19, 2017 regarding their FOIA request for Internet complaints, "[FCC employee Mike] Hennigan again reiterated that the ombudsperson had received a large volume of complaints and correspondence and said that

[176] *Id.* at ¶ 77.
[177] *Commissioner Sandoval 2015 Open Internet Ex Parte Comments*, *supra* note 7, at 68.
[178] *Id.*, at 67-68 (citing *Open Internet 2014 NPRM*, 29 F.C.C. Rcd. 5561, 5587).
[179] *In the Matter of AT&T Mobility, LLC.*, 30 F.C.C. Rcd. 6613 (2015).
[180] *Internet Freedom NPRM*, *supra* note 1, at 50 (citations omitted).
[181] *Id.*
[182] FCC, *In the Matter of Restoring Internet Freedom*, Order, WC Docket 17-108 (July 17, 2017), http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0717/DA-17-686A1.pdf.
[183] *Id.*

NHMC would receive documents as they became ready."[184] The FCC reported to ARS TECHNICA on August 22 regarding the 47,000 consumer complaints, 18,000 carrier responses, and 1,500 emails documenting interactions between the FCC ombudsperson and Internet users that "[w]e anticipate releasing another batch of documents by the end of the week and will release the remainder as soon as we can."[185] The ability of the public to examine those consumer complaints is vital to understanding the need for enforceable rules to protect the Internet's openness. The FCC's apparent failure to consider these complaints in its *NPRM*, to timely provide a FOIA response with evidence of these complaints, and to recognize the need for rules and jurisdiction to support enforcement and respond to complaints, evidences the FCC's arbitrary and capricious decision-making in this proceeding in violation of the APA.

The *Internet Freedom NPRM* recognizes that the 2015 Open Internet Order established both an informal complaint and a formal complaint process, and asks whether the FCC should modify the enforcement process should it keep or modify any Open Internet rules.[186] The FCC amended the *Internet Freedom NPRM* to recognize the one formal complaint filed under the 2015 Open Internet rules, and asked "[w]hat have been the benefits and drawbacks of the complaint procedures instituted in 2010 and 2015? [187] The FCC asked "[c]an we infer that parties heeded the Commission's encouragement to "resolve disputes through informal discussions and private negotiations" without Commission involvement, except through the informal complaint process,"[188] but did not mention the 47,000 informal complaints it had received.

The Code of Federal Regulations, 47 C.F.R. 1.41, specifically allows for the filing of informal requests for Commission action, providing "[e]xcept where formal procedures are required under the provisions of this chapter, requests for action may be submitted informally. Requests should set forth clearly and concisely the facts relied upon, the relief sought, the statutory and/or regulatory provisions (if any) pursuant to which the request is filed and under which relief is sought, and the interest of the person submitting the request." The FCC does not have the discretion to diminish the 47,000 informal complaints it received alleging violations or conduct inconsistent with the 2015 Open Internet Order because they were filed through the established regulatory process for informal complaints. It is arbitrary and capricious for the FCC to omit to mention them in the NPRM when the FCC makes the complaint process and jurisdiction a central issue in the *Internet Freedom NPRM*.

Neither does the FCC acknowledge the difficulties of its "formal complaint" proceeding including the filing fee which may inhibit the public from submitting formal complaints. Complaints against Common Carriers are governed by 47 C.F.R. 1.42, and subpart E of the Code of Federal Regulations. Without conducting a rulemaking to change the status of informal

[184] Comments of Voices Coalition for Internet Freedom, et. al., (WC Docket No. 17-108), at 46, July 19, 2017, https://ecfsapi.fcc.gov/file/107202424413478/Voices%20Coalition%20NN%20Comments%20-%20WC%20Docket%2017-108%20-%2007.19.2017.pdf.
[185] Jon Brodkin, Stop hiding 47,000 net neutrality complaints, advocates tell FCC Chair, Ars Technica, August 22, 2017, https://www.google.com/amp/s/arstechnica.com/tech-policy/2017/08/dont-kill-net-neutrality-before-making-complaints-public-groups-tell-fcc/%3famp=1.
[186] *Internet Freedom NPRM*, *supra* note 1, at ¶96 (citations omitted).
[187] *Id.*, at ¶98, n. 219 (citing Formal Complaint of Alex Nguyen, Docket No. 16-242, Bureau ID Number EB-16-MD-003 (filed July. 26, 2016)).
[188] *Id.*

complaints, the FCC is not entitled to wholesale afford informal complaints less weight or exclude them from the record of relevant proceedings because people used the regulatory process codified in the Code of Federal Regulations, 47 C.F.R. 1.41.

During my six year term as a CPUC Commissioner I met hundreds of people who had filed complaints at the California Public Utilities Commission, some through the "informal" complaint process to the Consumer Affairs Branch, and some who filed a formal complaint treated as an adjudicatory proceeding. Most of the people I talked to who filed an "informal" complaint through a letter to the CPUC said they filed a "complaint." They did not make a distinction between the informal or formal complaint process, neither were most aware of the different complaint paths. Each person filing a complaint, whether through methods the agency deemed "informal" or through the formal complaint mechanism the Commission created, wanted the CPUC to hear, analyze, and resolve their complaint. The FCC must treat with due respect those who use its codified "informal" complaint process. The FCC must make public and analyze the information from those complaints in this record before any decision could be adopted on the merits of the issue the FCC has put forth as the central issue in this proceeding: is FCC jurisdiction necessary to protect the Open Internet and consumers.

The FCC has not made public the 47,000 informal complaints despite the request public records act request NHMC submitted in May. Neither the public nor the FCC can complete the record of this proceeding without analyzing those complaints and the role of FCC Open Internet protection rules and jurisdiction in protecting Internet access and distribution. The record is incomplete without a meaningful opportunity for the public and the FCC to analyze those complaints. Any decision adopted without such analysis and public availability of the complaint data would be arbitrary and capricious, disrespect the codified complaint process in 47 C.F.R. 1.41, and be unsupported by the record.

The *Internet Freedom NPRM* proposes to eliminate the FCC ombudsperson role established in the 2015 Open Internet Order to facilitate response to consumer complaints about violations of the Open Internet rules. The FCC asks "[i]s the role of an ombudsperson necessary to protect consumer, business, and other organizations' interests when the Commission has a Bureau—the Consumer and Governmental Affairs Bureau (CGB)—dedicated to protecting consumer interests? Our experience suggests that consumers are comfortable working with CGB, and typically did not call on the ombudsperson specifically."[189] Yet, the FCC's NPRM contains no analysis of the public's use of the Ombudsperson evident in the 1,500 emails documenting interactions between the FCC ombudsperson and Internet users that the FCC has acknowledged but has yet to produce in response to a pending FOIA request.[190]

"Has the ombudsperson been called to action to assist in circumstances that otherwise could not have been handled by CGB?" the Internet Freedom asked?[191] The public cannot answer this question without the information the FCC should have already produced and analyzed about public use of the Ombudsperson, informal complaint data, and response to those

[189] *Id.* at ¶97.
[190] See *supra* text accompanying note 185.
[191] *Id.*

complaints. This question reflects arbitrary and capricious rulemaking when the FCC has failed to analyze the data it possesses relevant to the questions about the Ombudsperson role, the complaint process, and the need for enforceable rules. The 47,000 complaints received since the FCC adopted enforceable Open Internet rules and the 1,500 emails between the Ombudsperson and the public all show that enforceable rules and FCC jurisdiction over ISPs, not simply unenforceable promises by ISPs or principles with no enforcement authority, are necessary to protect the Open Internet.

During the course of the *Internet Freedom* rulemaking, several ISPs announced their policy not to engage in Internet blocking or throttling.[192] AT&T, Comcast, and Verizon professed commitment to the Open Internet, but expressed disagreement with the Title II legal classification of ISPs that makes Open Internet rules enforceable by the FCC.[193] Comcast filed comments in the *Internet Freedom* rulemaking opposing "anticompetitive paid prioritization," but urged "flexibility" for paid prioritization for medical needs or uses such as autonomous vehicles.[194] Verizon's comments recommend several guiding principles for "mass market Internet access services" stating "[w]e support rules that prevent providers from charging content suppliers a fee to deliver their Internet traffic faster than the Internet traffic of others where the result is harm to competition or consumers."[195]

Verizon argued that "[a]ny rule should therefore be careful to underscore that a prohibition on paid prioritization needs to be focused on the instance where a provider might slow a consumer's access to a particular website or application in favor of another, competing one. But consumers should also be able to choose to prioritize certain content or applications, where technologically practicable."[196]

Verizon's proposal recognizes the need to protect other consumers from degraded service due to paid prioritization and proposes to do so through FCC rules. Verizon proposes adopting a "flexible framework" and argues that, "Title II regulation is ill-suited to protecting "consumers' unfettered ability to access lawful Internet content of their choice over broadband Internet access networks."[197] Verizon's comments do not describe the contours of the flexible framework it envisions. Nor does Verizon discuss the legal basis for FCC adoption or enforcement of any

[192] *See, e.g.*, Comcast, Comcast Customers Will Enjoy Strong Net Neutrality Protections, Today and In the Future, April 26, 2017 ("We do not block, slow down, or discriminate against lawful content. *And we believe in full transparency...you'll know what our customer policies are*"), http://corporate.comcast.com/openinternet/open-net-neutrality; AT&T, Open Internet ( ) ("we have always supported an internet that is transparent and free from blocking, censorship and discriminatory throttling. But relying on 80-year old regulations to ensure these fundamental open internet principles does not make sense."), http://about.att.com/sites/open_internet; Verizon, A Real Time for Action, July 12, 2017 ("we respectfully suggest that real action will involve people coming together to urge Congress to pass net neutrality legislation once and for all." …[W]hile we agree with the goal of an open Internet, we do not think the answer is to impose 1930s utility regulation on ISPs.")
[193] *Id.*
[194] Jacob Kastrenakes, *Comcast Says It Should be Able to Create Internet Fast Lanes for Self-Driving Cars*, The Verge, July 17, 2017, https://www.theverge.com/2017/7/17/15985114/comcast-paid-prioritization-autonomous-cars
[195] Comments of Verizon, *In the Matter of Restoring Internet Freedom*, 17-208, at 4, July 17, 2017, https://ecfsapi.fcc.gov/file/10717390819816/2017%2007%2017%20Verizon%20comments%202017%20Open%20Internet%20Notice.pdf.
[196] *Id.* at 20.
[197] *Id.* at 37.

rules constraining paid prioritization or protecting Internet openness if the FCC does not classify ISPs as common carriers under Title II. The case Verizon brought, *Verizon v. FCC*, held that the FCC had no jurisdiction to enforce non-discrimination rules under Title I as those rules imposed *per se* Title II-type common carrier obligations on ISPs.[198]

BLOOMBERG reported that Bob Quinn, AT&T's Senior Vice-President for Federal Regulatory Affairs said in a press briefing that AT&T was "willing to have a discussion" about restrictions on paid prioritization.[199] "I think to make a hard and fast rule around that is probably not a good idea at this point in time," he said, citing autonomous vehicles and other cases where certain types of Internet traffic should be given priority. "We have supported a case-by-case approach. If there's anti-competitive or some kind of consumer harm, we've supported that that shouldn't be allowed."[200] AT&T's expression of its willingness "to have a discussion" about restrictions on paid prioritization runs counter to its opposition to the legal classification that makes enforceable rules that protect the open Internet by prohibiting discrimination such as paid prioritization.

The FCC must address whether medical or machine Internet uses such as autonomous vehicles can be addressed through specialized services authorized in the *2015 Open Internet Order*. The FCC in July 2017 expanded "the band that vehicle radars can operate to 5 GHz of spectrum" a decision intended to "improve lane departure warning, blind spot detection systems, automatic braking and pedestrian detection."[201] While autonomous vehicles may use the Internet in addition to radar, it is not axiomatic that such vehicles should have priority over all other Internet users, even medical, safety, voting, national security, or other uses.

Safeguards must be put in place requiring that autonomous vehicles not degrade other nearby Internet users. Failure to do so would lead to cyber-crashes where an autonomous vehicle drive-by could slow or block other Internet users if it appropriated Internet priority as it traveled. This dystopia serves neither autonomous vehicle users, nor all other Internet users, and harms safety and the public interest. The FCC should conduct a rulemaking to explore the Internet needs of autonomous vehicles and whether they can run through specialized services or separate networks to prevent degradation to and interference with other Internet users.

The FCC's *Internet Freedom NPRM* makes no attempt to explain why specialized services that protect other users from Internet quality degradation could not advance public safety and innovation. "The APA's requirement of reasoned decision-making ordinarily demands that an agency acknowledge and explain the reasons for a changed interpretation."[202] "An agency may not, for example, depart from a prior policy *sub silentio* or simply disregard rules that are still on the books."[203] ISP Industry Associations representing major ISPs

[198] *Id.*
[199] Joshua Brustein, *Comcast and AT&T Say They Support Open Internet With Caveats, The two internet providers are trying to muddy the debate over net neutrality*, BLOOMBERG, July 12, 2017, https://www.bloomberg.com/news/articles/2017-07-12/comcast-and-at-t-say-they-support-open-internet-with-caveats.
[200] *Id.*
[201] *Id.*
[202] *USTA v. FCC*, 825 F.3d 674, 706–07 (D.C. Cir. 2016) (citing *Verizon*, 740 F.3d at 636).
[203] *Id*. (citing *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515, (2009)).

acknowledged the importance of the record of prior FCC proceedings in their opposition to the motion to extend time to file reply comments and the relevance of that record to the 2017 Internet Freedom docket. They argued that "[A]ll stakeholders have had multiple opportunities to weigh in on the core issues in play here for over fifteen years across a range of public dockets, including Notices issued by the Commission in 2010 and 2014, as well as the instant NPRM."[204] If the FCC proposes to abandon its commitment to protecting Internet users from diminished service due to paid priority for some users, the Commission must provide adequate notice that this what it intends to do, analyze the record for both the current proceeding and the prior proceeding whose rules it seeks to repeal, and explain its rationale for the departure.

The FCC cannot adopt restrictions or rules on paid prioritization as some ISPs suggested or oversee paid prioritization as a regulator[205] unless the FCC classifies ISPs as common carriers under Title II. The FCC describes as its "lead proposal" [206] its proposition to "reinstate the information service classification of broadband Internet access service."[207] The FCC *Internet Freedom NPRM* mentions only in passing the D.C. Circuit's 2014 decision in *Verizon v. FCC*. Yet, in *Verizon*, the D.C. Circuit found unenforceable the rules the FCC had adopted in 2010 to protect against ISP blocking, throttling, and discriminatory conduct based on a Title I classification.[208] The *Internet Freedom NPRM* fails to discuss the limitations of *Verizon v. FCC* on FCC proposals to oversee as a regulator paid prioritization. Nor does it discuss the jurisdiction through which it could handle complaints about violations of Internet openness principles the FCC professes to embrace, or the legal basis for any enforcement of such principles.[209] This failure to analyze the relevant law and record constitutes arbitrary and capricious decision-making under the APA and.

The FCC queries whether ISPs should be allowed to exact priority payments at Internet Access points where traffic is exchanged and major content delivery services often establish arrangements to facilitate Internet traffic.[210] The *Internet Freedom NPRM* does not mention Internet "peering," a method to exchange Internet traffic.[211] Neither does the *NPRM* distinguish between peering or other traffic arrangements at the network level as compared to paid prioritization proposed at either the network or local level. Nor does the *NPRM* advance proposals to ensure that paid prioritization does not degrade Internet service for content providers, also known as "edge providers."[212]

---

[204] *Opposition To Motion For Extension Of Time*, *supra* note 68,
[205] *Internet Freedom NPRM*, *supra* note 1, at ¶ 85.
[206] *Id.* at ¶ 100.
[207] *Id.* at ¶ 24.
[208] *Verizon v. FCC*, 740 F.3d 623, 655-656.
[209] The FCC's proposal in the *Internet Freedom NPRM* also does not address the earlier *Comcast* decision in which the D.C. Circuit struck down the "principles" the FCC had adopted in lieu of actual rules. If the FCC reverts to "principles" instead of "rules", it runs into a different problem.
[210] *Id.* at ¶ 87.
[211] See Robert Frieden, *Conflict in the Network of Networks: How Internet Service Providers Have Shifted from Partners to Adversaries*, 38 HASTINGS COMM. & ENT L.J. 63, 64 (2016) ("Most ISPs bartered network access through a process known as peering in lieu of metering traffic and billing for network use.")
[212] *Id.* at 90 (arguing that regulators "should permit ISPs to negotiate and secure surcharges for traffic prioritization, [but] advocates for such arrangements should bear the burden of proving that they will not intentionally degrade service to ventures opting not to pay a premium. ISPs should not have the opportunity to create artificial congestion as a way to nudge or shove consumers and content providers to premium services."

The *NPRM* asks "[h]ow have marketplace developments impacted the incentive and ability, if any, of broadband Internet access service providers to engage in conduct that is contrary to the four Internet Freedoms?"[213] The *Internet Freedom NPRM* asks about the effect of paid prioritization on "startups and innovation."[214] The *NPRM* does not mention the gatekeeper role of ISPs[215] nor the needs of "edge providers" analyzed in detail in the *2015 Open Internet Order*.[216] The FCC's *2014 Open Internet NPRM* proposed to define "edge provider" as: "[a]ny individual or entity that provides any content, application, or service over the Internet, and any individual or entity that provides a device used for accessing any content, application, or service over the Internet."[217] My comments in that rulemaking pointed out that [i]n an age of telemedicine, interactive education, home-grown video, Facebook, email, the web, and other interactive services, whether novel, mundane, or critical to life, health, and safety, we are all edge providers."[218]

The ISP gatekeeper role was discussed at length in *Verizon v. FCC* which found that the "Commission also convincingly detailed how broadband providers' position in the market gives them the economic power to restrict edge-provider traffic and charge for the services they furnish edge providers."[219] The D.C. Circuit explained "[b]ecause all end users generally access the Internet through a single broadband provider, that provider functions as a "'terminating monopolist,' with power to act as a 'gatekeeper' with respect to edge providers that might seek to reach its end-user subscribers."[220] "As the Commission reasonably explained, this ability to act as a 'gatekeeper' distinguishes broadband providers from other participants in the Internet marketplace—including prominent and potentially powerful edge providers such as Google and Apple—who have no similar 'control [over] access to the Internet for their subscribers and for anyone wishing to reach those subscribers.'"[221]

The FCC's *Internet Freedom NPRM* fails to discuss the D.C. Circuit's conclusion in *Verizon v. FCC* that "[b]roadband providers also have powerful incentives to accept fees from edge providers, either in return for excluding their competitors or for granting them prioritized access to end users."[222] The Court emphasized that "at oral argument Verizon's counsel announced that "but for [the *Open Internet Order*] rules we would be exploring those commercial arrangements.""[223] The D.C. Circuit emphasized "[m]oreover, as the Commission found, broadband providers have the technical and economic ability to impose such

[213] *Internet Freedom NPRM*, *supra* note 1, at ¶ 77.
[214] *Id.* at ¶ 86.
[215] *2015 Open Internet Order*, 30 F.C.C. Rcd. 560, ¶¶ 20-21, 78, 80-81, 84, 97, 200, 444.
[216] *Id.* at 19-22, 24, 27, 29, 41, 43, 68, 75, 78, 80-85, 90-91, 96-97, 99, 103, 109, 113-115, 120, 127-129, 133, 135-138, 140, 142-144, 150-151, 154-155, 158, 161, 162-163, 164, 169, 172, 176-178, 181, 185, 193, 195-196, 198-203, 205, 226-227, 252, 266, 288-289, 294-295, 297, 306, 328, 338-339, 361, 364, 419, 431, 444, 540, 554, 559, 562-563, 569, 575, Appendix A, §§ 8.2(b), 8.11, Appendix B(2)(5)(8)(11)(12)(15), (61-62), (65-67).
[217] *Open Internet 2014 NPRM*, supra note 165, at Appendix A, 8.11(c).
[218] *Commissioner Sandoval 2015 Open Internet Ex Parte Comments*, *supra* note 7, at 11.
[219] Verizon v. F.C.C., 740 F.3d 623, 646.
[220] *Id.* (citations omitted).
[221] *Id.*
[222] *Verizon v. F.C.C.*, 740 F.3d 623, 645–46.
[223] *Id.*

restrictions."[224] The *Internet Freedom NPRM* discusses none of those findings underscored in *Verizon v. FCC* and the *2010 Open Internet Order*, or discuss similar findings in the *2015 Open Internet Order*, upheld in USTA v. FCC, 825 F.3d 674.

Instead, the *Internet Freedom NPRM* expresses skepticism about the incentive and ability of ISPs to engage in conduct which threatens the Internet's open nature. Incompass, an association of competitive communications providers, pointed out that "the Commission has made the question of the incentives and abilities of the broadband providers to harm the openness of the Internet a central question—perhaps the central question—in this proceeding."[225] Yet, Incompass argued, the Commission has compiled an insufficient record to assess this issue. Incompass moved for the FCC to compile "a complete record from evidence already available to the Commission … from formal transaction proceedings conducted by the Commission that looked squarely at the incentives and abilities of broadband providers to harm the open Internet."[226] As Incompass pointed out, the "Commission has an obligation under the APA to create a complete record."[227] Failing to do so would constitute reversible error.[228]

The Commission's failure to address in the *Internet Freedom NPRM* its prior extensive findings about ISP gatekeeper roles and concerns about ISP conduct that constrains "edge providers" constitutes arbitrary and capricious decision-making under the APA. "The APA's requirement of reasoned decision-making ordinarily demands that an agency acknowledge and explain the reasons for a changed interpretation."[229] "An agency may not, for example, depart from a prior policy *sub silentio* or simply disregard rules that are still on the books."[230] *Verizon v. FCC*[231] and *USTA v. FCC*[232] both upheld the FCC's findings in the 2010 and 2015 Open Internet orders about the gatekeeper roles of ISPs and concern about their ability to use their position on the Internet to the detriment of unaffiliated providers.

---

[224] *Id.*

[225] Incompass, Response to Oppositions to Motion of Incompas to Modify Protective Orders, (WC Docket No. 17-108), August 3, 2017, at 1-2, https://ecfsapi.fcc.gov/file/10804774408806/INCOMPAS%20Response%20to%20Oppo-3Aug.pdf.

[226] *Id.* at 2 (requesting in part unredacted versions of the FCC's orders for merger, transfer, and other transactions where the FCC examined the incentives and abilities of broadband providers to harm the open Internet including "underlying confidential or highly confidential information that the Commission cited and therefore relied upon in the orders").

[227] *Id.* at 7 (citing "*Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 30-31 (1983) (holding that agencies "must examine the relevant data," and the reviewing court "must consider whether the decision was based on a consideration of the relevant factors")); *see also Nat'l Black Media Coal. V. FCC*, 775 F.2d 342, 356 (D.C. Cir. 1985) ("[a]n agency has the duty to examine all 'relevant data'")).

[228] *Id.* (citing *Black Warrior Riverkeeper, Inc. v. US Army Corp. of Engineers*, 781 F.3d 1271, 1291 (11th Cir. 2015)).

[229] *USTA v. FCC*, 825 F.3d 674, 706–07 (D.C. Cir. 2016) (citing *Verizon*, 740 F.3d at 636).

[230] *Id.* (citing *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515, (2009)).

[231] *Verizon v. F.C.C.*, 740 F.3d 623, 646.

[232] *USTA v. FCC*, 825 F.3d 674, 711 (noting that in *Verizon v. FCC's* review of the *2010 Open Internet Order* the Commission also "convincingly detailed how broadband providers' [gatekeeper] position in the market gives them the economic power to restrict edge-provider traffic and charge for the services they furnish edge providers."); Id. at 694 (upholding the Commission's regulation of interconnection arrangements under Title II with forbearance in the *2015 Open Internet Order* noting that "[s]everal commenters, the Commission pointed out, had emphasized "the potential for anticompetitive behavior on the part of broadband Internet access service providers that serve as gatekeepers to the edge providers ... seeking to deliver Internet traffic to the broadband providers' end users.")

The FCC's *Internet Freedom NPRM* acknowledges that the "Commission partially justified the 2015 rules on the theory that the rules would prevent anti-competitive behavior by ISPs seeking to advantage affiliated content."[233] The FCC requests comment on whether these rules are necessary "in light of antitrust regulations aimed at curbing various forms of anticompetitive conduct, such as collusion and vertical restraints under certain circumstances."[234]

The FCC's question about the sufficiency of antitrust regulations to restrain anticompetitive conduct does not analyze the record finding that the ISP gatekeeper role can harm edge providers, all who provide content on the Internet. Neither does it recognize that antitrust and unfair competition laws would not *ex ante* prohibit practices such as blocking, throttling, and paid prioritization, or limit ISPs to reasonable and transparent network management practices.

Consumer protection statutes may address misrepresentations, disjunctions between ISP promises and practices, but cannot create forward-looking rules that protect Internet openness. Limited competition for high-speed Internet service inhibits the ability to shop around restrictive ISP practices including paid prioritization. The FCC found that most Americans have the choice of only one or two high-speed Internet providers. Customers unhappy with ISP policies may face early termination fees if they wish to cancel their contract "effectively penalizing a subscriber for the ISP's previously undisclosed practices and discouraging switching."[235] Customers may also encounter transaction costs or face higher prices if they transferred from one provider to another. These difficulties and costs are increased if the customer wishes to end Internet service from a provider from which it receives bundled service and a discount on several services sold with the bundle.

The FCC also fails to recognize that antitrust and unfair competition law remedies are available *only for injuries to competition*.[236] Antitrust and unfair competition regulations possess no authority to address harms to national security and democracy. Nor does the FCC acknowledge or address the harms of its proposals on national security, democracy, and American life – harms not compensable through antitrust laws. These omissions constitute an arbitrary and capricious departure, without adequate notice, reasoning, or analysis, from the Commission's prior decision-making.[237]

---

[233] *Internet Freedom NPRM*, *supra* note 1, at ¶ 78.
[234] *Id.* at ¶ 78.
[235] Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*, *supra* note 166, at 681.
[236] *Atlantic Richfield Co. v. USA Petroleum Co.*, 495 U.S. 328, 334 (1990), (holding that antitrust laws were intended to prevent and protect against "antitrust injury" "attributable to an anti-competitive aspect of the practice under scrutiny.")
[237] *FERC v. Electric Power Supply Ass'n*, ____U.S. ____, 136 S.Ct. 760, 784 (2016) ("When reversing existing policy, the Supreme Court has held that the APA requires an agency to provide more substantial justification when its new policy rests upon factual findings that contradict those which underlay its prior policy."); *Fox Television Stations, Inc. v. F.C.C.* 280 F.3d 1027, 1047 (D.C. Cir. 2002) (holding that the Commission's decision to retain the National Television Station Ownership rule was "arbitrary and capricious" and contrary to law" because the Commission failed to explain its departure from its previously expressed views."), *opinion modified on reh'g* (D.C. Cir. 2002) 293 F.3d 537.

The FCC's *Internet Freedom NPRM* lacks recognition of any risks from its proposals to allow unregulated paid prioritization. The FCC's credence in an unregulated market to protect the Open Internet is not tempered by any legal or factual analysis of the gatekeeper roles of ISPs over content providers. Neither does the FCC analyze the effect of the limited choices for high-speed Internet service that leave consumers unable to shop around restrictive policies, topics extensively discussed in the 2015 Open Internet Order.[238] Many comments submitted in this docket through the FCC's Express Comments portal underscore the limited choice for high-speed Internet service as a reason for supporting Title II classification and enforceable FCC rules to constrain ISP behavior. As the D.C. Circuit observed in overturning the Media Ownership rules in 2002 because of the FCC's failure to explain its departure from prior rulings, [t]his paean to the undoubted virtues of a free market in television stations is not, however, responsive to the question…"[239] The FCC's *Internet Freedom NPRM* fails to ask the relevant questions, propose any basis on which it could retain jurisdiction to address threats to Internet openness and complaints, and fails to analyze or explained the reasons for its proposed departure from previous decisions recognizing the need for enforceable rules to restrain ISP gatekeeper power.

The FCC's *NPRM* omits discussion of either the national security implications of paid prioritization or its consequences for American democracy. The *Internet Freedom NPRM* does not mention the words "democracy" or "national security." It mentions "security" only with reference to Federal Trade Commission (FTC) regulations to protect "privacy and security of consumer information."[240] The FCC fails to ask: "What happens to our democracy if candidates for political office or their supporters, domestic or foreign, could enter into undisclosed special deals for fast Internet access or thwart competing messages?" "How can we safeguard our democracy, economy, and national interest if no rules or laws prohibit ISP blocking, throttling, or paid prioritization and ISPs drop their voluntary policies not to engage in such practices."[241]

This omission ignores the Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21). That Directive orders the FCC to partner with the Department of Homeland Security, Department of State, other federal departments and sector-specific agencies on "identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities."[242] Adopted pursuant to the Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5291c, PPD-21 mandates that the FCC work with "stakeholders, including industry," and engage with "foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the

[238] See *supra* notes 215-218 and accompanying text.
[239] Fox Television Stations v. FCC, 280 F.3d 1027 (D.C. Cir., 2002).
[240] *Id.* at ¶ 93, note 201 (also noting that the no-blocking rule applies only to lawful content "and does not prevent or restrict a broadband provider from refusing to transmit unlawful material, such as child pornography or copyright-infringing materials").
[241] Sandoval, *Protect the Open Internet*, *supra* note 153.
[242] White House, Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), Additional Federal Responsibilities, 8, [adding in web banner that "This is historical material "frozen in time". The website is no longer updated and links to external websites and some internal pages may not work."], https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. This Directive has not been specifically supplanted or annulled.

Nation depends."[243] This directive requires that the FCC work with all stakeholders including industry and consumers − residential, business, government, non-profits, critical infrastructure providers, and others − to identify and address vulnerabilities to promote communications resiliency. This Presidential Directive, the Critical Infrastructure Protection Act of 2001, 42 U.S.C. 5291c, and President Trump's Executive Order on Cybersecurity and Critical Infrastructure requires more than meetings. The President's Executive Order underscore the national imperative of the FCC working to improve communications security, reliability, and resiliency, a paramount duty which continues in FCC rulemakings.

The Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5291c reflects Congress' finding that "[t]he information revolution has transformed the conduct of business and the operations of government as well as the infrastructure relied upon for the defense and national security of the United States."[244] That Act finds that "[p]rivate business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors."[245] The interdependency between critical services and communications services including the Internet has increased dramatically in the last 16 years. They are so intertwined that communications and Internet service are embedded in many critical sector services.

President Trump's Executive Order on Cybersecurity and Critical Infrastructure recognizes the critical role of Internet and communications services to Critical Infrastructure including energy. That Executive Order adopts as the policy of the Executive Branch "an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft."[246] An open and neutral Internet is essential to protect critical infrastructure such as the energy sector. The open Internet is vital to every American dependent on the energy, water, communications, police, fire, public safety, military, government, business, health, educational, and other services that rely on the open Internet.

C. The FCC's Proposals and Conduct of The *Internet Freedom* Proceeding Constitute Arbitrary and Capricious Decision-making under the APA.

The FCC *Internet Freedom NPRM* asks questions about, but makes no proposals for, a legal basis for FCC enforcement or complaint jurisdiction over ISPs other than the Title II classification the *2015 Open Internet Order* deemed necessary to support enforceable rules.[247] These questions do not substitute for proposals or provide sufficient notice under the APA. In *USTA v. FCC*, the D.C. Circuit determined that the FCC's *NPRM* for the *2015 Open Internet Order* satisfied the APA's notice requirements as it "described in significant detail the factors that would animate a new [general conduct] standard, though it didn't list the rules conduct.[248]

[243] *Id*.
[244] 42 U.S.C. 5195c (b)(1).
[245] *Id.*
[246] *Executive Order on Cybersecurity*, *supra* note 128, Sec. 3(a).
[247] *Id.* at ¶¶ 100-104.
[248] 825 F.3d 674, 735.

The FCC's *Internet Freedom NPRM* fails to describe in any detail the factors that would support the FCC's legal jurisdiction theory to respond to complaints, engage in enforcement, or oversee as a regulator paid prioritization if it adopts its "lead proposal" to reclassify ISPs under Title I of the Communications Act. The *NPRM* seeks comment on whether Section 706 of the Telecommunications Act of 1996, which directs the FCC and the states to take action to promote broadband deployment, is an affirmative grant of authority.[249] The *NPRM* does not propose to use Section 706 to support enforcement of open Internet principles or to respond to complaints, though that directive is routed in Title I, a classification *Verizon v. FCC* found inadequate to support non-discrimination rules or jurisdiction.

The *Internet Freedom NPRM* seeks "comment on whether section 230 [42 USC 230] gives us the authority to retain any rules that were adopted in the *Title II Order* [the *2015 Open Internet Order*]." The FCC noted that "the D.C. Circuit in *Comcast* speculated that "[p]erhaps the Commission could use section 230(b) . . . to demonstrate . . . a connection" to an "express statutory delegation of authority," although it had not done so there."[250] The *NPRM* asks, "[i]f the Commission were to demonstrate a connection to an express statutory delegation of authority, what would such a demonstration look like? What, if any, express statutory delegations of authority over broadband Internet access service exist?"[251] The FCC makes no proposals about which express statutory delegations of authority could support Open Internet rules or their enforcement and asks for comment about whether any exist. The D.C. Circuit observed a similar omission in *Comcast v. FCC*, "in this case the Commission cites neither section 230(b) nor section 1 to shed light on any express statutory delegation of authority found in [Communications Act] Title II, III, VI, or, for that matter, anywhere else."[252] The *Internet Freedom NPRM* does not provide sufficient notice under the APA of the range of choices under consideration to use section 230 as the jurisdictional foundation for Open Internet enforcement or complaint jurisdiction.

The APA requires the FCC do more than ask questions in a rulemaking about foundational issues such as the legal basis for overseeing ISP conduct to protect Internet openness. The APA mandates that the FCC make sufficiently specific proposals to create an opportunity for comment and response.[253] The D.C. Circuit stated in *Prometheus Radio Broad. v. FCC* that an agency must "describe the range of alternatives being considered with reasonable specificity. Otherwise, interested parties will not know what to comment on, and notice will not lead to better-informed agency decision-making."[254] The D.C. Circuit determined in *Prometheus* that the lack of notice of the range of alternatives being considered, coupled with irregularities in the comment process, supported the court's conclusion that the FCC failed to satisfy the APA and engaged in arbitrary and capricious rulemaking.[255] The FCC fails to "describe the range of alternatives being considered with reasonable specificity" to preserve its jurisdiction over ISPs

[249] *Internet Freedom NPRM, supra* note 1, at ¶ 101.
[250] *Id. (*referring to *Comcast Corp. v. FCC*, 600 F.3d 642, 654 (D.C. Cir. 2010)).
[251] *Id.*
[252] *Id.*
[253] *Council Tree Communications, Inc. v. Federal Communications Commission*, 619 F.3d 235, 249 ("if the substance of an agency's final rule strays too far from the description contained in the initial notice, the agency may have deprived interested persons of their statutory right to an opportunity to participate in the rulemaking.")
[254] 652 F.3d 431, 450 (citing *Horsehead Res. Dev. Co., Inc. v. Browner,* 16 F.3d 1246, 1268 (D.C.Cir.1994)).
[255] *Id.*

and respond to complaints about threats to Internet openness. This failure results in arbitrary and capricious rulemaking in violation of the APA and prevents the FCC from adopting rules in the Order to address these issues since it gave no notice of the contemplated rules.[256]

Under the APA, 5 U.S.C. § 553(b)(3), federal agencies must publish "either the terms or substance of the proposed rule or a description of the subjects and issues involved."[257] The APA requires that "the final rule the agency adopts must be 'a logical outgrowth' of the rule proposed.[258] *Verizon v. FCC* distinguished between common carrier rules that require non-discrimination, and rules such as the FCC's data roaming rule that "imposed no *per se* common carriage requirements because it left "substantial room for individualized bargaining and discrimination in terms."[259] The D.C. Circuit noted that the FCC's data roaming rule "expressly permit[ted] providers to adapt roaming agreements to 'individualized circumstances without having to hold themselves out to serve all comers indiscriminately on the same or standardized terms."[260] The *Internet Freedom NPRM* notes that *Verizon v. FCC* "suggested that no-blocking and no-unreasonable-discrimination rules might be permissible if Internet service providers could engage in individualized bargaining."[261]

The FCC's *Internet Freedom NPRM* does not propose to allow ISP "individualized bargaining" nor any parameters for such bargaining. The *2014 Open Internet NPRM* discussed in detail factors that would serve as strictures for "individualized bargaining" consistent with *Verizon v. FCC*, as an alternative to Title II classification.[262] My *ex parte* comments in the 2014-2015 Open Internet proceeding meticulously detailed concerns arising from the FCC's 2014 proposals for "individualized bargaining" under Title I arguing. My comments argued that these proposals were dangerous to public safety and harmed Internet openness. [263] The *2015 Open Internet Order* banned paid prioritization "based on the record that has developed in this proceeding" including "commenter concerns regarding preferential treatment arrangements, with

---

[256] *Prometheus Radio Broad. v. FCC*, 652 F.3d 431, 450 (requiring under the APA that an agency "describe the range of alternatives being considered with reasonable specificity. Otherwise, interested parties will not know what to comment on, and notice will not lead to better-informed agency decision-making")(citing *Horsehead Res. Dev. Co., Inc. v. Browner*, 16 F.3d 1246, 1268 (D.C.Cir.1994))).

[257] *Council Tree Communications, Inc. v. Federal Communications Commission*, 619 F.3d 235, 249 (3rd Cir. 2010).

[258] *Id.* (citing *Long Island Care at Home, Ltd. v. Coke*, 551 U.S. 158, 174 (2007) (quoting *Nat'l Black Media Coal. v. FCC*, 791 F.2d 1016, 1022 (2d Cir.1986))).

[259] Verizon v. F.C.C., 740 F.3d 623, 652 (citing *Cellco Partnership v. FCC*, 700 F.3d 534, 541 (D.C.Cir.2012)).

[260] *Id.* at 652.

[261] *Internet Freedom NPRM*, *supra* note 1, at ¶ 20 (citing Verizon v. F.C.C., 740 F.3d 623, 657) (quoting *Cellco Partnership v. FCC*, 700 F.3d 534, 549 (D.C. Cir. 2012))).

[262] *Open Internet 2014 NPRM*, *supra* 165, at 5593 ("we propose to adopt the text of the no-blocking rule that the Commission adopted in 2010, with a clarification that it does not preclude broadband providers from negotiating individualized, differentiated arrangements with similarly situated edge providers (subject to the separate commercial reasonableness rule or its equivalent). So long as broadband providers do not degrade lawful content or service to below a minimum level of access, they would not run afoul of the proposed rule. We also seek comment below on how to define that minimum level of service. Alternatively, we seek comment on whether we should adopt a no-blocking rule that does not allow for priority agreements with edge providers and how we would do so consistent with sources of legal authority other than section 706, including Title II.")

[263] *Commissioner Sandoval Notice of Ex Parte and Written Statement for the 2015 Open Internet Docket, supra* note 7, at 2, 3.

many advocating a flat ban on paid prioritization."[264] The *2015 Open Internet Order* noted that commenters argued that paid prioritization will introduce artificial barriers to entry, distort the market, harm competition, harm consumers, discourage innovation, undermine public safety and universal service, and harm free expression.[265] The FCC's *2015 Open Internet Order* cited my *ex parte* letter that paid prioritization will "undermine public safety and universal service."[266]

The California Public Utilities Commission echoed this concern in its 2017 comments supporting Title II classification for *ISPs*. The CPUC emphasized that "as the *2015 Open Internet Order* discusses, the absence of strong anti-discriminatory rules could undermine critical infrastructure and public safety."[267] Citing the FCC's reference to my *ex parte* letter raising concerns about the dangers of paid prioritization for public safety, the CPUC cautioned that "without non-discriminatory rules, providers of emergency services or public safety agencies might have to pay extra for their traffic to have priority. If states, cities, and counties were required to pay for priority access, their ability to provide comprehensive, timely information to the public in a crisis could be profoundly impaired."[268]

My *ex parte* comments and letter submitted for the 2015 Open Internet rulemaking discussed in detail why individualized bargaining proposals endanger critical infrastructure which relies on the open Internet for services such as energy demand response to prevent electrical blackouts.[269] Those comments highlighted the FCC's failure to discuss the "transaction costs" of individualized bargaining.[270] "For utilities with millions of customers such as Southern California Edison (SCE), an investor-owned electric utility (IOU) regulated by the CPUC, with over 4.9 million customer connections, negotiating Internet access agreements with multiple

---

[264] *2015 Open Internet Order*, 30 F.C.C. Rcd. 5601, 5653.
[265] *Id.* at 5654-5655 (citations omitted).
[266] *Id.* at 5654-5655, n. 291 (citing *Commissioner Sandoval ex parte letter supra* note 7, at 2 ("asserting that paid prioritization undermines public safety and universal service, and increases barriers to adopting Internet-based applications such as Internet-enabled demand response communications electric and gas utilities use to prevent power blackouts, forestall the need to build fossil-fueled power plants, promote environmental sustainability, and manage energy resources")).
[267] CPUC, Comments, *In the Matter of Restoring Internet Freedom*, at 29 (WC Docket No. 17-108) (July 17, 2017) (citing *2015 Open Internet Order*, 30 F.C.C. Rcd. 5601, ¶¶ 114, 126, 150. Paragraph 114 rejects the "minimum access standard" proposed to safeguard "individualized bargaining" from unduly degrading internet use. Paragraph 126 discusses the record support for barring paid prioritization based on comments including statements that paid prioritization risks degrading other users' access and can harm public safety and universal service. Paragraph 150 states that "[b]ased on the record before us, we are persuaded that adopting a legal standard prohibiting commercially unreasonable practices is not the most effective or appropriate approach for protecting and promoting an open Internet." That conclusion is based on record comments including those which raise concerns that a commercial reasonableness standard "would permit paid prioritization, which could disadvantage smaller entities and individuals."), https://ecfsapi.fcc.gov/file/107172199528427/WC%20Docket%20No.%2017-108%20CPUC%20Comments%20on%20Restoring%20Internet%20Freedom.pdf.
[268] *Id.* at 29 (citing the *2015 Open Internet Order*, 30 F.C.C. Rcd. 5601, at ¶ 126, noting commenters' concerns about paid prioritization and citing to an *ex parte* letter from then-CPUC Commissioner Catherine Sandoval, "asserting that paid prioritization undermines public safety and universal service….")
[269] *Commissioner Sandoval 2015 Open Internet Ex Parte Comments, supra* note 7, at 2, 3.
[270] *Id.* at 3 ("The FCC's Open Internet proposal does not even mention transaction costs, yet it subjects all Internet content providers ("edge providers") to closed negotiations with multiple ISPs to ensure that their messages get through and that others can reach them.")

ISPs to reach their 14 million customers would be costly, risky, and fraught with uncertainty."[271] The 2017 *Internet Freedom NPRM* likewise contains no discussion of the transaction costs of individualized bargaining such as the time, expense, delays, and power imbalances from *every* internet user having to individually bargain with their ISP for fast Internet access under rules that would explicitly permit discriminatory bargains. Neither does the *NPRM* propose any such rules. Instead, it leaves commenters to speculate about the contemplated basis for FCC complaint jurisdiction or regulatory oversight, creating a guessing game inconsistent with the APA.

The importance of the open Internet is illustrated by modern energy deployment and use. Today's energy ecosystem is increasingly characterized by distributed energy resources. Remote energy generators, whether renewable or fossil-fueled, Internet-connected devices at customer premises that can respond to energy grid operator calls to reduce power consumption to forestall blackouts, distribution and transmission monitoring, all depend on fast and reliable Internet access. It is critical to energy safety, reliability, and just and reasonable rates that Internet messages − whether initiated by customers, suppliers, energy generators, contractors, regulators, public officials or safety officers, local communities in the utility service territory, or at the utility's headquarters − not be subject to paid prioritization delays, payment demands, or service degradation due to priority accorded to other users who pay extra.

As a CPUC Commissioner, the FCC's *2015 Open Internet Decision's* adoption of enforceable Open Internet rules through Title II classification gave my colleagues and me confidence in the rules for regulatory oversight over ISPs. Enforceable rules that prohibited ISPs from blocking, throttling, or engaging in paid prioritization encouraged our decisions to authorize Internet-enabled investments by energy and water ratepayers. The CPUC's November 2016 Energy Savings Assistance Program (ESAP) Decision, for which I served as the Assigned Commissioner, approved state investments to help low-income Californians save energy in a manner that benefits all and reduces greenhouse gases.[272] The ESAP Decision approved ratepayer investment in several Internet-based services including those that leverage customer-facing programs such as funding "a smart thermostat that can participate in a demand response program, or a lighting control that can be internet enabled to track entry/exit behavior."[273] The CPUC 2016 ESAP Decision orders energy utilities and contractors to enroll customers who have an active email address and home or mobile Internet access in energy education programs, and to facilitate the ability of customers to use mobile or stationery computers to enroll in ESAP.[274]

The unanimous decision I authored providing guidance on water rates and tiers, D.16-12-026, ordered large investor owned water utilities in California to consider filing proposals for Advanced Metering Infrastructure (AMI) to improve water leak detection and harness data communication that benefits customers, saves water, and increases water sustainability and rate affordability. "Advanced metering infrastructure (AMI) is an integrated system of smart meters, communications networks, and data management systems that enables two-way communication

[271] *Id.*
[272] California Public Utilities Commission, Decision 16-11-022, Decision on Large Investor Owned Utilities' California Alternative Rates for Energy and Energy Savings Assistance Program Applications, (Nov. 21, 2016), http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M155/K759/155759622.PDF.
[273] *Id.* at 53.
[274] *Id.* at 171, 318.

between utilities and customers."[275] These networks facilitate multi-sided communication including customer access to information through the Internet. "Customer systems [that harness AMI] include in-home displays, home area networks, energy management systems, and other customer-side-of-the-meter equipment that enable smart grid functions in residential, commercial, and industrial facilities."[276] These decisions relied on the FCC's *2015 Open Internet Order's* Title II classification of ISPs to protect ratepayer investments in Internet-connected devices and platforms. Those investments, safeguarded by the *2015 Open Internet Order*, enable ratepayers to save water, a precious resource during times of drought, increase reliability, improve water quality and safety, and maintain just and reasonable rates.

The Internet Association's comments emphasize that "investment in the cloud economy has been booming since 2015."[277] "The cloud" has become increasingly important for data storage and making robust computing power available to a wide variety of users. The Internet Association emphasized:

> The economic data following the Commission's 2015 Order and net neutrality rules demonstrate that the Commission's analysis in its 2010 and 2015 Orders regarding maintenance of the virtuous circle of innovation and growth have remained true — clear rules of the road have given edgebased apps and services the certainty needed to attract investment and growth without being concerned about ISPs acting as gatekeepers, and the growth of these services has driven demand among consumers for faster and better broadband access, leading to continued growth in ISP investment and broadband subscriptions.[278]

The CPUC's decisions to authorize investment of energy and water utility ratepayer dollars in Internet-enabled apps and services to increase reliability, safety, and affordability are examples of the edge investments the *2015 Open Internet Order* spurred. Reclassification of ISPs as information service providers with no proposal for FCC enforcement or complaint jurisdiction leaves water, energy, and other rate-payers and members of the public at risk, and deters further investments in Internet-enabled services.

The *Internet Freedom NPRM* fails to propose a "particular change"[279] which would allow the FCC to respond to harms or consumer complaints resulting from its proposals. Nor does it provide "sufficient factual detail and rationale for the rule to permit interested parties to comment meaningfully."[280] The FCC proposes to repeal the Title II classification that enabled its complaint and enforcement jurisdiction. In its place the FCC proposes no rule or legal theory

[275] SmartGrid.gov, https://www.smartgrid.gov/recovery_act/deployment_status/sdgp_ami_systems.html.
[276] *Id.*
[277] Comments of Internet Association, at 16, July 17, 2017, WC Docket No. 17-108, https://ecfsapi.fcc.gov/file/10717274209550/IA%20Net%20Neutrality%20Comments%20Docket%2017-108%20F.pdf.
[278] *Id.*
[279] *USTA v. FCC*, 825 F.3d 674, 700.
[280] *Id.* at 712.

upon which it could base enforcement or respond to complaints to protect the "commitment to a free and open Internet" the NPRM professes to embrace.[281]

The legal classification of ISPs and FCC jurisdiction to respond to issues and complaints is what this rulemaking is all about. Nonetheless, the FCC makes no proposal for a legal basis that would confer jurisdiction to enforce any rules or help consumers, let alone protect American democracy or national security. This is not a harmless error.[282] An agency's "final rule would be considered arbitrary and capricious if the agency "entirely failed to consider an important aspect of the problem."[283]

Even if the FCC publishes its proposed *Internet Freedom* Order shortly before voting on it, the truncated time for review and brief comment period will prejudice the right to comment when the FCC has announced its likely judgment. The APA gives the public the right to comment on an agency's proposals as announced in an NPRM before they are developed into a tentative or final order. The D.C. Circuit's precedents in U.S. *Telecom Association*, *Prometheus* and *Horsehead* compel the conclusion that the use of only questions with no proposals for a legal foundation upon which to base enforcement of Open Internet rules or principles and failure to raise key issues resulting from its proposal constitutes a notice problem under the APA and reflects arbitrary and capricious decision-making.

My 2015 Open Internet *ex parte* comments emphasized that the "Internet is a vital component of the U.S. economy and society, and key to our nation's global economic competitiveness."[284] Those comments concluded: "To ensure a vibrant, competitive, open Internet, and that common carriers and interconnected VoIP providers and the customers they serve do not suffer undue discrimination, I support the FCC's reliance on § 706 ***and*** on Title II to reclassify the transport component of broadband access service as a telecommunications service with appropriate regulatory forbearance." The *2015 Open Internet* decision spurred Internet growth and investment in both infrastructure and edge services and applications that rely on the Internet's openness. Under the *2015 Open Internet Order*, content providers do not have to ask ISPs if they can launch or transmit data. Only Title II provides the legal foundation to protect that openness necessary to the virtuous cycle of innovation[285] the Internet enables.

---

[281] *Internet Freedom NPRM, supra* note 1, at ¶ 70 ("Proposing to restore broadband Internet access service to its long-established classification as an information service reflects our commitment to a free and open Internet.")

[282] *Cf., USTA v. FCC*, 825 F.3d 674, 725 ("A deficiency of notice is harmless if the challengers had actual notice of the final rule, *Small Refiner Lead Phase–Down Task Force v. EPA*, 705 F.2d 506, 549 (D.C. Cir. 1983), or if they cannot show prejudice in the form of arguments they would have presented to the agency if given a chance, *Owner–Operator Independent Drivers Ass'n v. Federal Motor Carrier Safety Administration*, 494 F.3d 188, 202 (D.C. Cir. 2007).")

[283] *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983); *People of State of Cal. v.* FCC, 4 F.3d 1505, 1511 (9th Cir. 1993) ("[I]f the record reveals that the agency has failed to consider important aspects of a problem or has offered an explanation for its decision that runs counter to the evidence before it, the court must find the agency in violation of the APA.").

[284] *Commissioner Sandoval 2015 Open Internet Ex Parte Comments*, *supra* note 7, at 95.

[285] *2015 Open Internet Order*, 30 F.C.C. Rcd. 5601, 5604 ("the *Verizon* court upheld the Commission's finding that Internet openness drives a "virtuous cycle" in which innovations at the edges of the network enhance consumer demand, leading to expanded investments in broadband infrastructure that, in turn, spark new innovations at the edge")(citing *Verizon v. FCC*, 740 F.3d 623, 659).

V. Conclusion

These Reply Comments support the comments and complaints of ordinary Americans who allege they have been victims of identity theft in the FCC's *Internet Freedom* rulemaking docket. The FCC must address false filing allegations by firmly stating that it does not tolerate criminal manipulation of its public decision-making process. This criminal conduct undermines the public input and comment systems that are the cornerstone of democratic decision-making.

The FCC, the FBI, and State Attorneys General must investigate and hold accountable those responsible for filing allegedly false comments using stolen identities in the *Internet Freedom* docket. Authorities must also determine whether persons or entities outside the United States including Russians are, in fact, filing comments in the *Internet Freedom* proceeding, or are engaging in misdirection or an influence operation. Investigators must determine whether the source of those comments is being spoofed or masked to deceive the FCC and the public. More analysis is needed of the "non-traditional" DDoS attack the FCC concluded bore markers of "potential malicious intent" "designed to impede the performance of the comment filing system's components." These activities must be examined in the context of the allegations of false filings based on stolen identities and data breaches. Each of these actions may be part of an influence campaign, not separate incidents.[286] State and federal law enforcement investigation is needed to determine the source – whether foreign or domestic – and motivations of the alleged false filings based on identity theft, data breaches, and bot swarm attacks in this proceeding.

State Attorneys Generals should investigate whether identity theft has been committed against their state residents in the FCC *Internet Freedom* proceeding. State Attorneys General have the legal authority and power to take appropriate steps to protect those whose purloined names and addresses are falsely displayed in unauthorized comments submitted in this proceeding. The federal government should partner with states to seek accountability for any criminal or unlawful civil conduct. Lacking such federal cooperation, states are imbued with the power and legal authority to investigate and prosecute criminals on their own.

The FCC must take down comments that victims allege are falsely filed without their authorization, and can do so by cooperating with the victims and State Attorneys General including obtaining victims statements sworn under penalty of perjury. Immediate action by the FCC and State Attorneys General is needed to protect the victims of identity theft in the *Internet Freedom* rulemaking. The FCC abrogates its responsibilities by allowing the ongoing perpetration of identity and false filings in this proceeding.

The FCC has announced no plan to investigate identity theft and false filing allegations or the source of those filings. Because the FCC has taken no steps to distinguish false from authorized comments, it cannot address this problem merely through the weight it gives or denies to express comments. The FCC's failure to consider the 47,000 public complaints about violations of the Open Internet rules before it published the *Internet Freedom NPRM* or during the comment period underscores the Commission's arbitrary and capricious conduct of this proceeding.

[286] Letter from Ajit Pai to Senator Wyden, *supra* note 36.

The FCC's 2015 Open Internet decision acknowledged the important role of public comment and its analysis of the content of those comments. "Congress could not have imagined when it enacted the APA almost seventy years ago that the day would come when nearly 4 million Americans would exercise their right to comment on a proposed rulemaking. But that is what has happened in this proceeding and it is a good thing."[287] "Public input has improve[d] the quality of agency rulemaking by ensuring that agency regulations will be 'tested by exposure to diverse public comment,'" the FCC noted in substantiating its conclusion that "[t[here is general consensus in the record on the need for the Commission to provide certainty with clear, enforceable rules."[288]

In sharp contrast, the FCC's 2017 rulemaking process has seemingly tolerated manipulation of public input through allegedly false filings. The FCC's order extending the reply comment period, the statements of Chairman Pai and FCC spokespersons indicate that the Commission is aware of the allegations of false filings, identity theft and database breaches, and that the agency itself has alleged a bot swarm hampered the comment filing process. Instead of raising alarm bells or acting to protect the integrity of its proceeding or the victims of identity theft, the FCC has neither committed to investigate these criminal allegations nor paused this proceedings to develop a record about the impact of this abhorrent conduct on its rulemaking proposals, licensees, or the public. This arbitrary and capricious decision-making manifests a bizarre indifference to the integrity of the Commission's process and the legal principles of democratic decision-making.

The FCC's procedural flaws are compounded by its failure to consider the impact of its proposals on national security and democracy, critical issues foundational to the FCC's statutory mission. The FCC's proposal to allow unregulated paid prioritization on the Internet reflects a September 11-level of failure of imagination about risks it poses to America's national security and democracy. The FCC proposes no limits on who could buy paid Internet priority. Neither does the Commission's proposal recognize that it would allow foreign governments or their agents to seek Internet priority in the United States, whether by purchasing it or creating incentives to hack devices and accounts to obtain that fast pass.

Sanctions form a limited deterrent as many sanctions only apply to named individuals or organizations or those working on behalf of a sanctioned government. The attractiveness of paid prioritization as a means to speed Internet messages to and across the United States increase incentives to circumvent sanctions. The FCC proposes no rules or jurisdiction to safeguard against degradation of other Internet users to accommodate those who pay for Internet priority. Priority status may degrade and even block the messages of America's citizenry, our government, military, and democratic institutions such as the press and educational institutions.

---

[287] Open Internet 2015 Decision, *supra* note 7, at ¶ 13, 80 FR 19738.

[288] Id., at ¶ 13, 80 FR 19739. *See also*, Sprint Corp. v. F.C.C. (D.C. Cir. 2003) 315 F.3d 369, 373 ("The notice requirement [of the APA] "improves the quality of agency rulemaking" by exposing regulations " 'to diverse public comment,' " ensures " 'fairness to affected parties,' " and provides a well-developed record that "enhances the quality of judicial review." *Small Refiner Lead Phase–Down Task Force v. United States EPA,* 705 F.2d 506, 547 (D.C.Cir.1983)).

.

Unregulated paid prioritization increases risks to cybersecurity, particularly in light of bot and other attacks that can subject Internet resources to the command of foreign or domestic criminals. The FCC's suggestion that it allow paid prioritization overseen by a regulator is undercut by its lead proposal to classify ISPs as information service providers, a category that removes FCC regulatory jurisdiction to enforce rules or respond to complaints. The D.C. Circuit's decision in *Verizon v. FCC* makes plain that only the Title II classification of ISPs can be used to support FCC rules or jurisdiction to respond to complaints about Internet openness. That jurisdiction and those bright line rules should be maintained and the FCC should withdraw its ill-conceived 2017 proposal.

The Internet has evolved since the 2003 speech then-FCC Chairman Powell gave about the four Internet freedoms that led to unenforceable rules to protect the Internet's open nature.[289] Since the *2015 Open Internet Order*, the Internet has become more integrated into American life. Proliferation of the Internet of Things and development of edge services including cloud services have accelerated that integration and the Internet's growth under the protection of the rules adopted in the FCC's 2015 Open Internet Order. The Internet, American democracy, and national security are intertwined and face new challenges in the short time since the *2015 Open Internet Order's* adoption.

The *Countering America's Adversaries Through Sanctions Act* made a Congressional finding that "[o]n January 6, 2017, an assessment of the United States intelligence community entitled, "Assessing Russian Activities and Intentions in Recent U.S. Elections" stated, "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the United States presidential election.""[290] That intelligence warns "Moscow will apply lessons learned from its Putin-ordered campaign aimed at the U.S. Presidential election to future influence efforts worldwide, including against U.S. allies and their election processes."[291] That campaign was carried out in significant part through the Internet. The *Countering America's Adversaries Through Sanctions Act* codified Executive Order No. 13694 (blocking the property of certain persons engaging in significant malicious cyber-enabled activities), and Executive Order No. 13757 (taking additional steps to address the national emergency with respect to significant malicious cyber-enabled activities), in recognition of the increasing cyber threats to America.[292]

The intelligence community assessment and report of foreign interference with U.S. elections was publicly known by the May 23, 2017 date of the *Internet Freedom NPRM's* publication. Yet, the *NPRM* fails to acknowledge or address the changing threats to America's cybersecurity, democracy, economy, and national security. Neither does the FCC recognize the risks of its proposals to American security, even as the agency acknowledges "bot swarm" attacks show "potential malicious intent" to interfere with the comment and governmental

[289] *Internet Freedom NPRM*, *supra* note 1, at 5, n. 36 (citing Michael K. Powell, Chairman, Federal Communications Commission, Preserving Internet Freedom: Guiding Principles for the Industry, Remarks at the Silicon Flatirons Symposium (Feb. 8, 2004) (announcing Internet Freedom principles including "the freedom to access lawful content, the freedom to use applications, the freedom to attach personal devices to the network, and the freedom to obtain service plan information"), https://apps.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf.

[290] *Countering America's Adversaries Through Sanctions Act*, *supra* note 9, §211 (6).

[291] *Id.*

[292] *Id.* at 222(a).

decision-making process.[293] Allegations of false filings based on identity theft and data breaches underscore the changed circumstances this proceeding must address, and the new threats to the Open Internet we must confront. Law enforcement authorities and the FCC should explore whether the identity theft and false filings in this rulemaking are linked to the increasing cyber threats America faces. Sadly, for this FCC rulemaking, the prospect of foreign involvement in false filings based on data breaches and identity theft is not the stuff of spy novels. These are real issues, criminal conduct allegations, the FCC, state, and federal law enforcement authorities must address. Congressional findings signed into law through the *Countering America's Adversaries Through Sanctions Act*[294] indicate that the cybersecurity ground has shifted.

These Reply Comments highlight the dangers of the FCC's proposals to remove ISP regulation and jurisdiction in light of Congressional findings of foreign "influence operations" that harness the Internet. The FCC's failure to consider the implications of its proposals for national security and democracy demonstrates arbitrary and capricious decision-making under the APA. Moreover, these proposals put America at risk. Enforceable rules are needed now more than ever as a bulwark against interference with Internet access or legal Internet content distribution.

The FCC was created in 1934 "to make available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communications…."[295] Chaos on the airwaves reigned prior to the enactment of the Communications Act of 1934. At the dawn of broadcasting "new stations used any frequencies they desired, regardless of the interference thereby caused to others. Existing stations changed to other frequencies and increased their power and hours of operation at will."[296] The Supreme Court observed the "result was confusion and chaos. With everybody on the air, nobody could be heard."[297] The Supreme Court later found in a seminal case that reviewing FCC spectrum regulation that "[w]ithout government control, the medium would be of little use because of the cacophony of competing voices, none of which could be clearly and predictably heard.[298]

The FCC's proposal to remove both its rules and jurisdiction over ISPs would create a cacophony on the Internet, allowing those who can pay for priority to push ahead of others so only those with priority can be heard. This cyber-Mad Max version of the Internet would allow those with paid or hacked priority to push other Internet communications to the back of the line or make their connection attempts fail. This is the type of communications dystopia the FCC was founded to prevent. In omitting analysis of the implications of its proposals for the national defense, promoting life and safety, and democracy, the FCC fails to execute its statutory charge.

---

[293] Letter from Ajit Pai, Chairman FCC, to Senator Ron Wyden, *supra* note 36.
[294] *Countering America's Adversaries Through Sanctions Act*, *supra* note 9, §211 (6).
[295] 47 USC 151.
[296] *National Broadcasting Co. v. U.S.*, 319 U.S. 190, 212 (1943).
[297] *Id*.
[298] *Red Lion Broadcasting Co. v. F.C.C.*, 395 U.S. 367, 376 (1969).

Repeal-without-replace proposals to "consider rolling back these rules" while hoping "for Congress to take action and create regulatory and economic certainty"[299] would eliminate the FCC's authority to respond to complaints and threats to the Internet's openness. In that void Internet users and content suppliers would face unchecked ISP control without resort to federal government rules or complaint jurisdiction. The potential for foreign interference in an unregulated American Internet raises concerns for our national security, economy, and democracy. As President Trump recognized in his Executive Order on Cybersecurity,[300] the open Internet is critical to our economy, democracy, national security, and society.

The FCC should withdraw this *NPRM* in light of the criminal manipulation of the comment process. The FCC's failure to investigate leaves it unable to discern authorized from false filings based on identity theft, indicating arbitrary and capricious decision-making. The FCC must consider the risks to national security, democracy, and our economy its proposals create. The FCC can avoid creating an Internet dystopia and protect American national security and democracy by withdrawing its proposals while law enforcement examines the rampant criminal conduct apparent in this proceeding.

The FCC's conduct of this proceeding indicates a pervasive infection of the FCC's process and its incomprehensible tolerance of apparent criminal conduct. As the D.C. Circuit stated in *Office of Communications of the United Church of Christ v. FCC*, "The record now before us leaves us with a profound concern over the entire handling of this case…"[301] The FCC cannot shake this off by discounting public comment when it has conducted no investigation to discern authentic from authorized comments. The FCC's failure to consider the record and rationale for the 2015 Open Internet rules and the negative consequences of its 2017 proposals for American national security and democracy render any decision the FCC would make in this proposal arbitrary and capricious.

Thank you for your consideration of these Reply Comments which are based on public sources and my analysis of the FCC's *Internet Freedom NPRM* and the record including the legal requirements to avoid arbitrary and capricious decision-making. Omission of discussion of other issues raised by the NPRM should not be seen as agreement, disagreement or waiver of any position related to those issues. I reserve the right to file additional comments.

Sincerely,
/////s/////////
Catherine Sandoval
Associate Professor
Santa Clara University School of Law

[299] Brian Fung, *supra* note 12.
[300] *Executive Order on Cybersecurity*, *supra* note 128, Sec. 3(a) ("To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft.")
[301] Office of Communication of United Church of Christ v. F.C.C., 425 F.2d 543, 550.