~~FRAUDULENT~~ MALATTRIBUTED COMMENTS IN AGENCY RULEMAKING

Michael Herz†

TABLE OF CONTENTS

† Arthur Kaplan Professor of Law, Benjamin N. Cardozo School of Law, Yeshiva University. Many thanks to Bridget Dooling, Cynthia Farina, Jonathan Rusch, and Felix Wu for extremely helpful comments on an earlier draft and to Joshua Bressman and Alec Kirschenbaum for their excellent research assistance.

INTRODUCTION

A specter is haunting notice-and-comment rulemaking—the specter of fraudulent comments.[1] The stand-out example—the apotheosis—was the Federal Communications Commission's (FCC) net neutrality rulemaking in 2017. Well over *twenty million* comments were submitted, but millions of those were highly suspect. It turns out only about 800,000 of those comments were unique—that is, not written by a computer and not a pre-written form letter or variation thereof.[2] And of the rest, perhaps half were submitted by computers (bots) using fictitious names or the names of real people, living and dead, who had no connection to the comment. As described by (dissenting) Commissioner Jessica Rosenworcel:

> [W]hen the agency made the misguided decision to roll back its net neutrality rules, it did so based on a public record littered with problems. While millions of Americans sought to inform the FCC process by filing comments and sharing their deeply-held opinions about internet openness, millions of other filings in the net neutrality docket appear to be the product of fraud. As many as nine and a half

1 "Fraudulent" is the standard term. As this article's title implies, I understand its attraction but think it is not quite right. *See infra* Section IV.A.

2 Ryan Singel, *Filtering Out the Bots: What Americans Actually Told the FCC About Net Neutrality Repeal*, STAN. CTR. FOR INTERNET & SOC'Y BLOG (Oct. 15, 2018, 6:00 AM), http://cyberlaw.stanford.edu/blog/2018/10/filtering-out-bots-what-americans-actually-told-fcc-about-net-neutrality-repeal [https://perma.cc/ZZ78-HHMW].

> million people had their identities stolen and used to file fake comments, which is a crime under both federal and state laws. Nearly eight million comments were filed from e-mail domains associated with FakeMailGenerator.com. On top of this, roughly half a million comments were filed from Russian e-mail addresses.
>
> Something here is rotten—and it's time for the FCC to come clean.[3]

That sounds *terrible*. And, indeed, judging by the furious and strident reaction, fraudulent comments are a catastrophe. On this account, these comments are harmful at two levels. On the one hand, they destroy the integrity of agency decision-making; the outcome of a notice-and-comment process crammed with fraudulent comments—"corrupted by endemic fraud"[4]—is at least suspect if not simply invalid per se. And on the other hand, millions of individuals are being harmed through a form of "identity theft." Pennsylvania Attorney General Josh Shapiro stated: "The theft of someone's voice in our democracy cannot stand, and we must get to the bottom of this massive identity theft. That is a compelling reason the FCC should not press forward with its action to rollback Net Neutrality rules."[5] And all of this is not simply bad, it is illegal. The very terms "fraudulent comments" and "identity theft" state legal conclusions.

I will suggest that this reaction is over-wrought and rests on a fundamental misconception of the nature of notice-and-comment rulemaking. There is nothing good about fake comments; we should not celebrate them; there is no silver lining; agencies should take steps to prevent or weed out such submissions to the extent they can do so without discouraging legitimate comments. But neither are they actually all that harmful, either to the agency or to the individuals whose names have been used. And despite the frequent and easy assertions of illegality, it is not at all clear that any law is being violated. To borrow Cynthia

---

3 Nicholas Confessore and Jeremy Singer-Vine on Request for Inspection of Records, 33 FCC Rcd. 11808 (Adopted Nov. 7, 2018) (Rosenworcel, dissenting).

4 Prechtel v. FCC, 330 F. Supp. 3d 320, 332 (D.D.C. 2018).

5 Courtney Linder, *Pennsylvania AG Josh Shapiro Joins Lawsuit Against the FCC Over Net Neutrality Rollback*, PITTSBURGH POST-GAZETTE (Jan. 16, 2018), http://www.post-gazette.com/business/tech-news/2018/01/16/josh-shapiro-fcc-net-neutrality-lawsuit-pennsylvania-ajit-pai/stories/201801160126 [https://perma.cc/9CH8-FX92].

Farina's memorable analogy: fake comments are like pink eye; they look really terrible but are not actually that big a problem.[6] Anxieties about *other* cyber threats that resemble fake comments have made people hypersensitive in this quite different setting. Threats such as Russian interference with American elections, bot-disseminated disinformation on social media platforms, and identity theft are very serious problems with very real consequences for society and affected individuals. Fake comments look like those problems and stir the same unease. But they are just not the same.

I. THE PROBLEM

In December 2017, the *Wall Street Journal* published a lengthy article by James Grimaldi and Paul Overburg[7] reporting on work they had done over several months looking into the docket for the FCC's net neutrality rulemaking.[8] This was a giant rulemaking with a record number of public comments: almost twenty-five million.[9] The focus of the article was not that astonishing and unprecedented total, but on the large number of duplicative, mass, and, most of all, phony (i.e. submitted under a false name) comments. "They included comments from stolen

---

6 Cynthia Farina, Remarks at the Administrative Conference of the United States and Administrative Law Review Symposium: Mass and Fake Comments in Agency Rulemaking 119 (Oct. 5, 2018), https://www.acus.gov/sites/default/files/documents/10-5-18%20Mass%20and%20Fake%20Comments%20in%20Agency%20Rulemaking%20Transcript.pdf [https://perma.cc/VFP3-264D].

7 James V. Grimaldi & Paul Overburg, *Millions of People Post Comments on Federal Regulations. Many Are Fake.*, WALL ST. J. A1 (Dec. 13, 2017).

8 In 2015, the FCC issued its "net neutrality rule," classifying broadband Internet as a "telecommunications service." That classification carries with it common carrier obligations, and the rule prohibited broadband Internet providers from blocking, degrading, or interfering with Internet traffic. Protecting and Promoting the Open Internet, 80 Fed. Reg. 19737 (June 12, 2015). The rule was upheld in *United States Telecomm. Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016). In 2017, the FCC proposed repealing the 2015 rule. In the Matter of Restoring Internet Freedom, WC Docket No. 17-108. The Notice of Proposed Rulemaking was released in May and published in the *Federal Register* in June. 82 Fed. Reg. 25,568 (June 2, 2017).

9 The comment period ran to July 17; the reply period ended August 17. As is typical with FCC rulemakings, comments continued to flow into the docket well after the nominal deadlines had passed. As of September 25, 2018, the docket contained 23,951,747 total filings. *Docket 17-108*, FCC, https://www.fcc.gov/ecfs/search/filings?proceedings_name=17-108&sort=date_disseminated,DESC [https://perma.cc/S5VP-XSXZ].

email addresses, defunct email accounts and people who unwittingly gave permission for their comments to be posted. Hundreds of identities on fake comments were found in an online catalog of hacks and breaches."[10] A consulting firm later determined that more than a million comments came through a pornographic website; a third of the comments, 7.75 million, were sent from temporary or disposable email domains through FakeMailGenerator.com; about 10 million were from senders of multiple comments.[11] The whole thing was a shambles, Exhibit A for those who view electronic commenting as a farce.

The *Journal* article received a huge amount of attention and prompted a number of follow-up stories from many outlets. But the problem had been perceived well before December. Already in May 2017, then New York Attorney General Eric Schneiderman had launched an investigation. By his count, the FCC docket included eight million submissions with "fabricated" identities and one million with "stolen" identities.[12] Schneiderman and his Pennsylvania counterpart, Josh Shapiro, both created web pages for individuals to report that phony comments had been submitted to the FCC under their names.[13] Each of

---

10 Grimaldi & Overburg, *supra* note 7. A video on the newspaper's website summarizes:

> [T]he *Wall Street Journal* uncovered thousands of comments from fake email addresses, abandoned or defunct email accounts, posted on behalf of unwitting participants. For example, 818,000 identical comments on the FCC site favor repealing the rules. In a random sample of people whose emails were used for those posts, 72% said they had nothing to do with them. Jack Hirsch was one of them. "I was horrified. Knowing that this is actually an issue that I cared enough to write my representatives about, and knowing that my information had been falsified to support a completely opposing view, it was really frustrating, and honestly, I felt like there was no recourse.

Thousands of Fake Comments on Net Neutrality: A WSJ Investigation, WSJ | VIDEO (Dec. 12, 2017, 12:02 PM), https://www.wsj.com/video/thousands-of-fake-comments-on-net-neutrality-a-wsj-investigation/8E52172E-821C-4D89-A2AA-2820F30B8648.html [https://perma.cc/7DH4-QLT7].

11 EMPRATA, FCC RESTORING INTERNET FREEDOM DOCKET 17-108: COMMENTS ANALYSIS 2 (2017), https://www.emprata.com/emp2017/wp-content/uploads/2017/08/FCC-Restoring-Internet-Freedom-Comments-Analysis.pdf [https://perma.cc/VVH2-TRSP].

12 Letter from Eric Schneiderman, Att'y Gen., N.Y., to Thomas M. Johnson, Jr., Gen. Counsel, FCC (Dec. 13, 2017), https://ag.ny.gov/sites/default/files/ltr_to_fcc_gen_counsel_re_records_request.pdf [https://perma.cc/T3WE-ZTZR].

13 *Fake Comments*, N.Y. ST. OFF. OF THE ATT'Y GEN., https://ag.ny.gov/fakecomments [https://perma.cc/FJZ6-R72X]; *Fake FCC Comments*, OFF. OF THE ATT. GEN.—JOSH SHAPIRO,

the sites links to the FCC docket, making it easy to search for one's own name among the comments. The user can then fill out a simple form confirming that her name was used by someone else, indicating the comment number, and stating whether a current or past address was used in the comment and, "[i]f you have an opinion about whether Title II net neutrality rules should be left in place or repealed, did the comment match that view or was it the opposite of your actual view?"[14]

The FCC Open Internet rulemaking was the most visible and extreme example of an electronic docket containing comments that were computer-generated and/or purporting to be from an individual who had nothing to do with the submission. But the phenomenon is more widespread than just this one rulemaking. Grimaldi and Overburg reported on phony comments in rulemakings conducted by the Consumer Financial Protection Bureau, Federal Energy Regulatory Commission, and the Securities and Exchange Commission.[15]

Not surprisingly, politicians took notice. They responded in two ways. First, and most intensely, opponents of the repeal of the net neutrality rule latched on to the defects in the notice-and-comment process in an effort to derail the rulemaking altogether. Many argued that the process was so compromised that the FCC had to delay or wholly

---

https://badcomments.attorneygeneral.gov [https://perma.cc/H584-TAWK]. As of July 22, 2020, the New York page is still up; the Pennsylvania page has been removed.

14 That phrasing is from the New York site. *Fake Public Comments Investigation*, N.Y. ST. OFF. OF THE ATT'Y GEN., https://ag.ny.gov/fakecomments-form [https://perma.cc/9UQJ-UUTW]. The Pennsylvania site asks whether "[t]he fake comment(s) I found: Matched my real view, Is/are opposite of my real view, I don't know / I have no view on net neutrality." *Fake FCC Comments*, *supra* note 13.

15 Grimaldi & Overburg, *supra* note 7. Though my focus is on notice-and-comment rulemaking, identical phenomena occur in other settings where mass online comments are invited. One prominent example is the process of producing an environmental impact statement (EIS), which involves public comment on a draft EIS (DEIS) prior to issuance of the final EIS. For example, a number of comments endorsing a massive Alaska mine have been submitted as comments on the DEIS in the name of, and with the email address of, the Natural Resources Defense Council (NRDC) attorney who is the project's most prominent opponent. *See* Dylan Brown, *Lead NEPA Story: Fake Comments vs. Form Letters in Pebble fight*, GREENWIRE (June 13, 2019), https://www.paep.org/wp-content/uploads/2019/09/National_Desk_June-21-2019.pdf [https://perma.cc/M9KE-N3ZL]. These submissions raise exactly the same issues as the comments discussed in this article.

abandon the rulemaking.[16] The FCC was unmoved. Dismissing the objections, it went ahead with the repeal. In its view, the pseudonyms just did not matter; what counted was the *content* of the submissions, not the signature line.[17]

Second, many lawmakers have voiced deep concerns. As mentioned, several state attorneys general (AGs) began investigations. In addition, in December 2017, several members of the House requested the Government Accountability Office (GAO) to investigate the FCC rulemaking as well as "any other rulemaking processes you deem appropriate for this review."[18] The letter sought investigation of "the prevalence of outside parties generating comments to federal rulemakings by utilizing false or stolen identities," possible violations of federal law, and the adequacy of mechanisms agencies have in place to prevent such submissions.[19] GAO agreed to undertake the investigation, anticipating that it would get underway in May 2018.[20] An overlapping group of Representatives, led by Frank Pallone and Elijah Cummings, wrote Attorney General Jeff Sessions and FBI Director Christopher Wray,

---

16 *See, e.g.*, Letter from Ellen F. Rosenblum, Oregon Att'y Gen., et al. to FCC (Dec. 13, 2017), https://www.doj.state.or.us/wp-content/uploads/2017/12/ag_letter_12-13-2017.pdf [https://perma.cc/PUE3-SB9J] (urging the FCC to delay the proceeding in order to investigate the "tainted comments") [hereinafter State AGs' Letter].

17 *See, e.g.*, Letter from Ajit Pai, FCC Chairman, to Representative Michael E. Capuano (Apr. 12, 2018), https://docs.fcc.gov/public/attachments/DOC-350373A1.pdf [https://perma.cc/LZQ5-BBWY] ("Despite any suggestion that the public comment process was somehow 'flawed' or 'tampered with' by the alleged submission of comments under false names, any such activity did not affect the Commission's actual decision-making . . . ."); Letter from Thomas M. Johnson, Jr., FCC Gen. Counsel, to Eric Schneiderman, N.Y. Att'y Gen. (Dec. 7, 2017), https://cdn.arstechnica.net/wp-content/uploads/2017/12/FCC-General-Counsel-Response-to-NYAG.pdf [https://perma.cc/HH2X-A2NF] ("[T]he Commission does not make policy decisions merely by tallying the comments on either side of a proposal to determine what position has greater support, nor does it attribute greater weight to comments based on the submitter's identity.").

18 Letter from Representative Gregory Meeks et al. to Honorable Gene Dodaro, Comptroller Gen. (Dec. 4, 2017), https://meeks.house.gov/sites/meeks.house.gov/files/wysiwyg_uploaded/12-5-17%20Meeks%20Letter%20to%20GAO%20on%20Misuse%20of%20Identities%20in%20Comment%20Process_0.pdf [https://perma.cc/7GPG-JHGF].

19 *Id.*

20 Letter from Orice Williams Brown, GAO, to Representative Frank Pallone (Jan. 9, 2018) https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Pallone_Redacted.pdf [https://perma.cc/L6AQ-BLNT].

also seeking an investigation.[21] There has been no formal response. And multiple members of Congress wrote to FCC Chairman Ajit Pai requesting a delay in the rulemaking. The FCC declined to slow things down. In the preamble to the final Order, and then in a series of ex-post letters to individual Members from Chairman Pai, it argued that the automated and phony comments did not undermine the process in any way and so there was no justification for delay.

On the Senate side, the Permanent Subcommittee on Investigations of the Committee on Homeland Security and Governmental Affairs launched an investigation, leading to a staff report[22] and a hearing.[23] The thrust of the report is that agencies must be far more vigilant and aggressive in ensuring that rulemaking documents contain real comments from real people, free of profanity or private information.

Meanwhile, agencies were and are considering how they can protect their dockets from phony comments. In March 2018, the Consumer Financial Protection Bureau (CFPB) issued a Request for Information

---

21 Pallone wrote in June 2017 and again in early 2018. Letter from Representative Frank Pallone et al. to Jefferson Sessions, Att'y Gen., and Christopher Wray, Dir. of the FBI (Jan. 24, 2018), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/DOJ.FBI_.2018.01.24.%20Letter%20on%20Fake%20Agency%20Comments.%20DCCP.CAT_Redacted.pdf [https://perma.cc/9AE9-GKZZ]. The letter states:

> The practice of manipulating agency actions by flooding rulemaking dockets with fake comments is far more widespread than it appeared when you were initially asked to investigate. Some Americans' voices are being co-opted in what appears to be a systemic attempt to corrupt federal policy-making.
>
> Immediate action is needed in order to restore public trust in the federal rulemaking process. We urge you to use the full investigative powers of the FBI and DOJ to promptly uncover who is behind this conduct and prosecute the parties under applicable federal law.

22 UNITED STATES SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, ABUSES OF THE FEDERAL NOTICE-AND-COMMENT RULEMAKING PROCESS 3 (2019) https://www.hsgac.senate.gov/imo/media/doc/2019-10-24%20PSI%20Staff%20Report%20-%20Abuses%20of%20the%20Federal%20Notice-and-Comment%20Rulemaking%20Process.pdf [https://perma.cc/83A5-YDZC]. The Report catalogues a range of related concerns with contemporary commenting, including mass comments, the use of profanity in comments, publication of information that is private, copyrighted, or trade secrets, and malattributed submissions.

23 *Review of E-Rulemaking Comment Systems, Joint Hearing Before Perm. Subcomm. on Investigations and the Subcomm. on Regulatory Affairs and Federal Management*, 116th Cong. (2019), recording and transcript available at https://www.govinfo.gov/content/pkg/CHRG-116shrg38895/pdf/CHRG-116shrg38895.pdf [https://perma.cc/39C6-62ZP].

regarding many aspects of its rulemaking process; one specific item on which it sought feedback was the "processing and posting of comments received to its electronic docket on *regulations.gov*, including . . . treatment of anonymous comments [and] treatment of comments where there may be questions about the commenter's identity."[24] Of the 152 comments received, almost none addressed this issue. A single submission—from the Consumer Bankers Association—referred to "media accounts [that] have reported disturbing abuses of the comment process in an attempt to controvert the federal rulemaking process."[25] I have no idea what it means to "controvert" the rulemaking process, but it sounds bad. (It is possible that the Association meant "subvert," which is also bad.)[26] It urged the CFPB to require commenters to register, to post only authenticated comments, and to prohibit anonymous comments, because "the benefits of providing an unmoderated forum are outweighed by the risks posed by fraudulent letters."[27]

Despite this upset, those voicing concerns never really articulate *why* they are so concerned. The Consumer Bankers Association refers to "the risks posed by fraudulent letters" but never reveals what those risks are. They are assumed to be self-evident. But it is impossible to determine whether particular kinds of comments undermine the process, or how much effort is worth expending in fighting them, without first understanding the nature and extent of the harm they cause. And to do that, it is necessary to have some theory of the purposes of notice and comment. Much (not all) of the perceived harm from "fraudulent

---

24 Request for Information Regarding Bureau Rulemaking Processes, 83 Fed. Reg. 10437, 10440 (Mar. 9, 2018).

25 Dong Hong, Consumer Bankers Ass'n, Comment, Docket No. CFPB-2018-0009-0079, https://www.regulations.gov/document?D=CFPB-2018-0009-0079 [https://perma.cc/53DW-3MJK].

26 In a letter to the FCC, Senator Richard Blumenthal and two colleagues referred to "concerns that the rule-making process was subverted by fraudulent comments and manipulated by special interests." Letter from Sens. Richard Blumenthal, Brian Schatz, & Edward Markey, to David Hunt, FCC Inspector General (Oct. 29, 2018), https://www.blumenthal.senate.gov/imo/media/doc/2018.10.29%20-%20FCC%20-%20Fake%20Comments.pdf [https://perma.cc/49EM-8VFG].

27 Hong, *supra* note 25. It is surely not a coincidence that such rules could meaningfully discourage individual and small business commenters but would have no impact on trade groups such as, for example, the Consumer Bankers Association.

comments" comes from a misunderstanding of the notice-and-comment process. If this were an election, we should be horrified at this corrupting and devastating stuffing of the ballot box. If this were someone's bank account, we should be horrified at the outright theft by the imposter (and the person whose identity was used would suffer a very tangible harm). If this were a visible public forum, then there might be some reputational harm to the impostee (if there is such a word). If the *contents* of the comments were problematic and being read by and influencing large swathes of the public, or impressionable children, or scientists (political or other) gathering data, we might be worried about the pollution of important information streams. But notice-and-comment rulemaking is none of those things.

The following sections consider how under a proper understanding of the process the harms from so-called fraudulent comments are quite dilute.

II. TERMINOLOGY

First, the matter of terminology. What should we call a comment filed under the name of someone who did not in fact prepare, approve, or submit it? The most common term is "fraudulent comment."[28] But this states a legal conclusion, a conclusion that, as I discuss below, is misplaced. The term is just inaccurate. It is also overbroad: a comment might be "fraudulent" in the sense of misleading or dishonest in *lots* of ways besides being submitted under a bogus name—most obviously, by making false assertions or relying on invented data. That is also a potential problem, but it is not the problem this Article (or the firestorm over the FCC rulemaking) is about.

An alternative is "fake comment."[29] But this too is inaccurate. These submissions do have something fake about them, but they are not fake

---

[28] *See, e.g.*, *Mass, Computer-Generated, and Fraudulent Comments*, Administrative Conference of the United States, https://www.acus.gov/research-projects/mass-computer-generated-and-fraudulent-comments [https://perma.cc/8KBA-7UUL].

[29] *See, e.g.*, *Fake Comments*, *supra* note 13; Kevin Collier & Jeremy Singer-Vine, *Millions of Comments About the FCC's Net Neutrality Rules Were Fake. Now the Feds Are Investigating*, BUZZFEED NEWS (Dec. 8, 2018, 1:20 PM), https://www.buzzfeednews.com/article/kevincollier/feds-investigation-net-neutrality-comments [https://perma.cc/T53C-FSZA].

comments; they are undeniably actual, real comments. They respond to a rulemaking proposal; they are submitted to the rulemaking docket; they state a view and/or contribute some information; there is no reason to think that that view is anything other than the view of the person who is actually submitting the comment. A "fake comment" might be something that is not actually a comment—say someone sent a chocolate bar to the agency for submission to the docket, labeling it a "comment." Or it might be disingenuous; an intentionally silly or ineffective or self-defeating comment that argued *against* the actual position of the submitter so ineffectively as to undermine the position it purported to take. That could be a "fake" comment. But these are actual comments, supporting the positions favored by the submitter.

"Pseudonymous comment" captures the essential fact that the problem is that the stated name of the submitter is not the actual name of the submitter. But it is overbroad; only a subset of pseudonymous comments is potentially problematic. The Internet is full of pseudonymous activity; users have screen names, avatars, aliases. Much of that activity is benign if not valuable; using a pseudonym is not necessarily misleading and often drives or enables valuable activity. Someone using a pseudonym can have a distinct, known, and identifiable voice and produce work of astonishing value. Think of Publius or George Eliot.

Another possibility is "fabricated comments."[30] This is closer. That captures an essential point—that there is something phony or manufactured about the comments—without overstating the point or asserting a legal conclusion. But it too is overbroad for our purposes. Comments can be fabricated in many ways; the term would also serve as a (tendentious and pejorative) label for mass comment campaigns, for Astroturf comment campaigns, and for computer-generated anonymous comments.[31]

---

[30] *See, e.g.*, *Fake It Till They Make It: How Bad Actors Use Astroturfing to Manipulate Regulators, Disenfranchise Consumers and Subvert the Rulemaking Process, Hearing Before the Oversight & Investigations Subcomm. of the House Committee on Financial Services*, 116th Cong. (Feb. 6, 2020) (prepared statement of Bartlett Collins Naylor, Public Citizen).

[31] These are related but distinct phenomena. A mass comment campaign involves a single organizing entity, often an NGO or other membership organization, urging its members or supporters to submit comments and, often, making it easy to do so by providing a prepared text and a hyperlink to the rulemaking docket. The result is generally multiple, sometimes tens of

Cary Coglienese has suggested the term "inauthentic comments."[32] That strikes my ear as better than "fabricated" but suffering from the same shortcoming; moreover, "inauthentic," like "fake," implies that the submission is not really a comment when in fact it is intended to influence public policy and there will be people who agree with its substance.

"Misattributed" is more promising. It highlights the particular problem: the commenter is attributing the comment to a person who did not write or submit it. It is a little anodyne; it also does not fit exactly because "misattribution" can be in good faith and is generally not done by the author. Still, I was going to go with that until Cynthia Farina suggested "malattributed."[33] The fact that "malattributed" is not actually a word in the English language undeniably counts against it. But the neologism has compensating benefits. Resonating with "malware" (and possibly "maladministration")[34] it communicates the submitter's bad

---

thousands, of essentially identical submissions. *See* Cynthia R. Farina, Paul Miller, Mary J. Newhart, Claire Cardie, Dan Cosley, Rebecca Vernon, & Cornell eRulemaking Initiative, *Rulemaking in 140 Characters or Less: Social Networking and Public Participation in Rulemaking*, 31 PACE L. REV. 382, 416 (2011). Astroturfing, a term generally attributed to Texas Senator Lloyd Bentsen, refers to an orchestrated effort, often bought and paid for, designed to look like it arose spontaneously from the grass roots. *See* John McNutt & Katherine Boland, *Astroturf, Technology and the Future of Community Mobilization: Implications for Nonprofit Theory*, 34 J. SOC. & SOC. WELFARE 165, 167 (2007) ("[Astroturf efforts] create the impression that local people are engaged in the effort and doing the things that traditional community organizations do."). Computer-generated comments are exactly that; multiple individual submissions that are not in fact from individual submitters but instead from a single computer source or bot. Each of these is potentially problematic, and the categories can merge and overlap, but none involves the key characteristic that is the focus of this article: submitting a comment that purports to be from someone who has nothing to do with it.

32 Cary Coglienese, Remarks at the Administrative Conference of the United States and Administrative Law Review Symposium: Mass and Fake Comments in Agency Rulemaking 106 (Oct. 5, 2018), https://www.acus.gov/sites/default/files/documents/10-5-18%20Mass%20and%20Fake%20Comments%20in%20Agency%20Rulemaking%20Transcript.pdf [https://perma.cc/VFP3-264D].

33 Email from Cynthia Farina to Michael Herz (Aug. 8, 2020) (on file with author).

34 At the Constitutional Convention, George Mason proposed "maladministration" as the ground for impeachment of the President. James Madison objected that that term covered too much conduct that did not justify removal from office, at which point Mason abandoned "maladministration" and proposed "high crimes and misdemeanors." 1 MAX FARRAND, THE RECORDS OF THE FEDERAL CONVENTION OF 1787, at 550 (rev. ed. 1937). My view of "malattributed comments" is similar, *mutatis mutandis*. They are to be regretted but are not so serious as to justify a ferocious response, being well shy of high crimes and misdemeanors.

intent while still focusing on the specific problem. So unless and until someone comes up with something better, that is the term I shall use.

III. IT'S NOT A VOTE!

In 2016, the Russian government and its agents engaged in a stealth disinformation campaign through social media in an effort to swing the presidential election.[35] For example, they created phony Facebook groups and pages focused on hot-button, divisive issues and purchased thousands of Facebook ads, put up event pages to encourage attendance at anti-immigrant rallies, and spread false stories of voter fraud.[36] Similar efforts were undertaken on Instagram. The key player here was the Internet Research Agency (IRA), a private company of "professional trolls"[37] linked to the Russian government. IRA Facebook posts reached 140 million users.[38] According to the Special Counsel's February 2018 indictment of the IRA and others, the agency "registered and controlled hundreds of web-based email accounts hosted by U.S. email providers under false names so as to appear to be U.S. persons and groups."[39]

These efforts caused justifiable anger and dismay. They almost certainly involved federal criminal violations. They had the potential of

---

35 Useful overviews include P.W. SINGER & EMERSON T. BROOKING, LIKEWAR: THE WEAPONIZATION OF SOCIAL MEDIA (2018).

36 SIVA VAIDHYANATHAN, ANTISOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY 87–89, 175–78 (2018).

37 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT U.S. ELECTIONS 4 (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [https://perma.cc/7Y96-54XA].

38 Jonathan Masters, *Russia, Trump, and the 2016 U.S. Election*, COUNCIL ON FOREIGN REL. (Feb. 26, 2018), https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election [https://perma.cc/98G7-AVEM].

39 Indictment ¶ 40, United States v. Internet Research Agency, No. 1:18-cr-00032-DLF (D.D.C. Feb 16, 2018). The indictment named the IRA, two other organizations, and thirteen Russian individuals as defendants. The prosecution has completely stalled. The individual defendants and the IRA have not responded, and remain, unreachable in Russia. The two other defendants unsuccessfully sought to dismiss the indictment, and aggressively sought sensitive information in discovery, leading the prosecution to move to dismiss the charges. Katie Benner & Sharon LaFraniere, *Justice Dept. Moves to Drop Charges Against Russian Firms Filed by Mueller*, N.Y. TIMES (May 7, 2020), https://www.nytimes.com/2020/03/16/us/politics/concord-case-russian-interference.html [https://perma.cc/M8U4-8UMT].

causing, and may well have caused, real harm by interfering with the legitimate electoral process.

Reports of Russian interference first surfaced in the summer of 2016, with news stories concerning the hacking of Democratic National Committee emails. In September, Democrats Dianne Feinstein and Adam Schiff, the ranking members of the Senate and House Intelligence Committees, issued a joint statement saying that they believed that Russian intelligence agencies were carrying out a plan to interfere with the election.[40] After the November election, press coverage began to cover the social media efforts, which were a major focus of press coverage throughout 2017.

Russian efforts to sway the 2016 election through manipulation of social media and bogus accounts are only the most visible of a raft of similar efforts that amount to "war by other memes."[41] One of the most disorienting and frightening aspects of our age is the frequency and effectiveness with which anonymous or pseudonymous social media accounts are used to spread disinformation.[42]

This is the background to the *Wall Street Journal* article about the net neutrality rulemaking. Read against a drumbeat of stories about Russian election hacking, a flood of computer-generated comments feels like more of the same. All the more so because Russian bots were the source of some of the phony comments.[43] Indeed, FCC Commissioner

---

40 Press Release, Dianne Feinstein, Feinstein, Schiff Statement on Russian Hacking (Sep. 22, 2016), https://www.feinstein.senate.gov/public/index.cfm/2016/9/feinstein-schiff-statement-on-russian-hacking [https://perma.cc/S3QJ-PQDX].

41 SINGER & BROOKING, *supra* note 35, at 17.

42 *See generally id.*; VAIDHYANATHAN, *supra* note 36.

43 James V. Grimaldi & Paul Overberg, *Millions of People Post Comments on Federal Regulations. Many Are Fake.*, WALL ST. J. (Dec. 12, 2017), https://www.wsj.com/articles/millions-of-people-post-comments-on-federal-regulations-many-are-fake-1513099188 [https://perma.cc/32ZP-JKFL] (quoting FCC spokesman Brian Hart as stating that over 400,000 comments in favor of the old rules came "from the same address in Russia"); Hamza Shaban, *FCC Commissioner, NY Attorney General Call for Delay of Net Neutrality Vote Over Fake Comments*, WASH. POST: THE SWITCH (Dec. 3, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/12/04/fcc-commissioner-new-york-attorney-general-call-for-delay-of-net-neutrality-vote-over-fake-comments [https://perma.cc/ZGG5-3UXL].

Jessica Rosenworcel made the link explicit in a *Washington Post* op-ed entitled "Russians Are Hacking Our Public-Commenting System, Too."[44]

However, the two settings are just not the same. The net neutrality rulemaking, like all rulemakings, was not an election. *Had it been,* then the phony comments would have been outrageous. Indeed, they would have been worse than the election interference. That was designed to *influence* voters; here, the phony comments were actual "votes." It would be election fraud on an unprecedented scale, millions of false votes. And false votes are problematic because they carry exactly the same weight as valid votes. Stuffing ballot boxes produces outcomes that are indisputably wrong and illegitimate because the right and legitimate outcome is exclusively a function of the vote tally. One cannot evaluate the correctness or legitimacy of the result of an election outcome except as a function of (a) full and fair procedures allowing all eligible voters to participate and (b) the final tally. The right outcome is the one a majority of voters support. That is precisely why actual voter suppression and actual voter fraud (if you can find it) must be taken seriously. Not counting votes or counting the wrong votes produces, by definition, the wrong outcome.[45]

Notice-and-comment rulemaking is a very different creature. Comments are not votes. The "right" and "legitimate" outcome is a function of the law, the facts, and reasoned decision-making. Duplicative comments are not especially helpful. Not everyone needs to participate. It is emphatically not a one-person, one-vote regime where all voices have equal weight. Some comments are more influential than others for entirely legitimate reasons—they are more complete, better-reasoned, more on point, or from a submitter with especially useful knowledge.

Since rulemaking began to move online two decades ago, many, including yours truly, have predicted, and lamented, that the result would

---

44 Jessica Rosenworcel, *Russians Are Hacking Our Public-Commenting System, Too*, WASH. POST (March 6, 2018, 4:37 PM), https://www.washingtonpost.com/opinions/russians-are-hacking-our-public-commenting-system-too/2018/03/06/fdfe3dae-1d6a-11e8-b2d9-08e748f892c0story.html [https://perma.cc/84FC-VDP2].

45 For a fuller, and more sophisticated, summary of electoral legitimacy, see James A. Gardner, *Democratic Legitimacy Under Conditions of Severely Depressed Voter Turnout*, U. CHI. L. REV. ONLINE (June 26, 2020), https://lawreviewblog.uchicago.edu/2020/06/26/pandemic-gardner/ [https://perma.cc/D6PS-F9FL].

be a shift to a model of notice-and-comment as a referendum.[46] For the most part, that prediction has not come to pass. To be sure, lay participants in notice-and-comment rulemaking tend to view it as a vote. This is one of the basic findings of Cynthia Farina and her Regulation Room colleagues. As they write:

> Rulemaking 2.0 takes place at the intersection of two powerful cultural patterns. The first is the popular equation in the United States of democratic voice with casting a vote, or, it's [sic] privatized equivalent, responding to a poll. Because voting is how "public participation" is culturally constructed, site visitors already "know" how the public provides input in government decision-making. Everyone "understands" that the side with the most votes wins. The second pattern is from online culture: Voting is how the Web works. Ranking or rating—by assigning stars, sliding a bar, or simply clicking "Like" or "Recommend"—is a staple of Web 2.0 interactivity. Like the gladiators of ancient Rome, web content lives or dies by whether the crowd gives thumbs up, or down. The confluence of these two patterns may create such a powerful "voting instinct" that the presence of even fairly modest preference-aggregation devices causes users to ignore other signals that they really ought to learn more about how rulemaking works.[47]

The powerful impulse to view notice-and-comment as a vote is reinforced by many mass comment campaigns. Repeatedly, those encouraging others to submit comments stress the need to show "support" for agency proposals they like or "opposition" to those they do not. Sometimes, the pitch is franker: "Whoever gets the most letters in wins."[48] Similarly, news accounts frequently emphasize how many

---

46 *See* Michael Herz, *Rulemaking*, *in* DEVELOPMENTS IN ADMINISTRATIVE LAW AND REGULATORY PRACTICE 2002–2003, at 148–49 (Jeffrey S. Lubbers ed., 2004).

47 Cynthia R. Farina, Mary J. Newhart, Claire Cardie, Dan Cosley, & Cornell eRulemaking Initiative, *Rulemaking 2.0*, 65 U. MIAMI L. REV. 395, 431–32 (2011) (citations omitted).

48 Holly Turner, *SEC Proxy Firm Rule* at 4:42, YOUTUBE (Jan. 3, 2020), https://www.youtube.com/watch?v=_zLAvx5JAZk&feature=youtu.be [https://perma.cc/5GV7-J8NX]. This video is controversial. *See, e.g.*, *Republican Operative Holly Turner Posts Appallingly Deceptive Video in Support of Anti-Shareholder Proposal from the SEC*, VALUEEDGE BLOG (Jan. 10, 2020), https://valueedgeadvisors.com/2020/01/10/republican-operative-holly-turner-posts-appallingly-deceptive-video-in-support-of-anti-shareholder-proposal-from-the-sec

comments support or oppose a proposal.[49] But in the eyes of the agencies,[50] the courts,[51] and commentators, notice-and-comment is not a

---

[https://perma.cc/27GW-GJBN]. As of September 29, 2020, it had fifteen thumbs down and fourteen thumbs up, which is encouraging in a glass-half-full kind of way.

49 *See, e.g.*, Jeff St. John, *Edison Electric Institute Declines to Support Petition Seeking Federal Overturn of Net Metering*, GREEN TECH MEDIA (June 4, 2020), https://www.greentechmedia.com/articles/read/edison-electric-institute-wont-endorse-petition-seeking-federal-overturn-of-net-metering [https://perma.cc/2BPC-84WD] (reporting, in a section of the article headed "No public support for NERA's anti-solar petition," that "[a]s of Thursday, no comments supporting NERA's petition had been filed in FERC's proceeding. But the docket is filled with comments opposing its legal argument").

50 REGULATIONS.GOV, TIPS FOR SUBMITTING EFFECTIVE COMMENTS 2, http://www.regulations.gov/docs/Tips_For_Submitting_Effective_Comments.pdf [https://perma.cc/XZL9-KB4P] ("The comment process is not a vote. The government is attempting to formulate the best policy, so when crafting a comment it is important that you adequately explain the reasoning behind your position."); *see also id*. at 3 ("Many in the public mistakenly believe that their submitted form letter constitutes a 'vote' regarding the issues concerning them. Although public support or opposition may help guide important public policies, agencies make determinations for a proposed action based on sound reasoning and scientific evidence rather than a majority of votes. A single, well supported comment may carry more weight than a thousand form letters."); Dylan Brown, *Fake Comments vs. Form Letters in Pebble Fight*, GREENWIRE (June 13, 2019), https://www.eenews.net/greenwire/stories/1060571783 (reporting on pseudonymous comments, many ad hominem and abusive, filed by project supporters to counter-balance environmentalist mass comment campaigns and quoting agency official as saying that "'substantive' comments are the only ones that matter anyway. 'It's really not like a vote.'").

51 *See, e.g.*, Hillsdale Envtl. Loss Prevention, Inc. v. U.S. Army Corps of Eng'rs, 702 F.3d 1156, 1181 (10th Cir. 2012) ("[W]e consider the substance of the comments, not the number for or against the project."); Alto Dairy v. Veneman, 336 F.3d 560, 569 (7th Cir. 2003) (Posner, J.) ("The purpose of a rulemaking proceeding is not merely to vote up or down the specific proposals advanced before the proceeding begins, but to refine, modify, and supplement the proposals in the light of evidence and arguments presented in the course of the proceeding."); U.S. Cellular Corp. v. FCC, 254 F.3d 78, 87 (D.C. Cir. 2001) (noting that the agency "has no obligation to take the approach advocated by the largest number of commenters; indeed, the Commission may adopt a course endorsed by no commenter" (citations omitted)); NRDC v. EPA, 822 F.2d 104, 122 n.17 (D.C. Cir. 1987) ("The substantial-evidence standard has never been taken to mean that an agency rulemaking is a democratic process by which the majority of commenters prevail by sheer weight of numbers. Regardless of majority sentiment within the community of commenters, the issue is whether the rules are supported by substantial evidence in the record. The number and length of comments, without more, is not germane to a court's substantial-evidence inquiry." (citations omitted)). Arguably, the strongest indicators that courts do not view notice-and-comment rulemaking as a referendum are what they have *not* said and arguments that litigants have *not* made. Agencies frequently reach a conclusion that runs counter to the majority sentiment of commenters. But those challenging the rule never argue that this fact means the rule is invalid. No one would think that is a winning argument. And because the

vote, a referendum, or a plebiscite. As Jennifer Nou has summed it up: "[A]gencies can't promulgate regulations by reference to how loudly the crowd applauds. They need evidence and facts."[52]

One silver lining of the net neutrality contretemps is that it reminds us of one reason (among several) why notice-and-comment should not be understood as a vote: it is a terrible way to aggregate preferences since it is utterly unrepresentative, non-random, and subject to manipulation.[53] If comments were votes, we would be in deep trouble even if the problem of bot-generated and malattributed comments was completely solved. In other words, *even if* it made sense for agencies to defer to, or consider, public sentiment, counting comments is not the way to do it. It is the exact opposite of something like deliberative polling, lacking the two essential features of that method: a random selection of participants and a process of education and discussion to insure informed votes.[54] If deliberative polling is the gold standard,[55] notice-and-comment

argument is not made, courts are never called upon to reject it. This is true even in extreme cases. For example, in 2003 the FCC adopted new rules about concentrated media ownership. Public comment on the proposal ran overwhelmingly against the proposal; approximately 99.9% of the almost two million comments were opposed. But the agency sided with the .1%. *See* Report and Order and Notice of Proposed Rulemaking, 2002 Biennial Regulatory Review—Review of the Commission's Broadcast Ownership Rules, 18 FCC Rcd. 13,620 (2003). *See generally* Mary M. Underwood, Comment, *On Media Consolidation, the Public Interest, and Notice and Agency Consideration of Comments*, 60 ADMIN. L. REV. 185 (2008). In the ensuing court challenge, the court did mention that it was "notabl[e]" that "nearly two million people weighed in by letters, postcards, e-mails, and petitions to oppose further relaxation of the rules." Prometheus Radio Project v. FCC, 373 F.3d 372, 386 (3d Cir. 2004). But it did not deem that fact legally relevant and nothing in its review turned on the number or one-sidedness of the comments.

52 Jennifer Nou, *The FCC Just Received a Million Net-Neutrality Comments. Here's What It's Like to Sort Through Them All*, WASH. POST (July 18, 2014, 6:00 AM), https://www.washingtonpost.com/posteverything/wp/2014/07/18/the-fcc-just-received-a-million-net-neutrality-comments-heres-what-its-like-to-sort-through-them-all [https://perma.cc/M5XZ-674P].

53 This irrefutable point is effectively made by, among others, Cynthia R. Farina, Mary Newhart, & Josiah Heidt, *Rulemaking vs. Democracy: Judging and Nudging Public Participation That Counts*, 2 MICH. J ENVTL. ADMIN. L. 123, 142–45 (2012).

54 *See generally* JAMES S. FISHKIN, WHEN THE PEOPLE SPEAK: DELIBERATIVE DEMOCRACY AND PUBLIC CONSULTATION (2009); James S. Fishkin, *Consulting the Public through Deliberative Polling*, 22 J. POL'Y ANALYSIS & MGMT. 128 (2003).

55 Jane Mansbridge, *Deliberative Polling as the Gold Standard*, 19 GOOD SOC'Y 55, 55 (2010) ("The Deliberative Polls of James Fishkin and Robert Luskin represent today the gold standard of attempts to sample what a considered public opinion might be on issues of political importance.").

rulemaking is the lead, or plastic, or thin-air standard. Even if we could ensure that every comment came from a real, single, unique submitter, there is no reason to think that the sum of yeas and nays would reflect overall public opinion.

It is easy to fake a vote; it is impossible to fake a useful comment. Sure, a comment that contained made-up data would look useful and turn out not to be. But the point is that the value of a comment turns on its *content*. That value can range from zero (useless) to, say, one hundred (fantastic). The value of a vote turns on its *source*; that value is either zero or one hundred. As long as agencies focus on the content of comments rather than their source or their numbers, malattributed comments are an annoyance but not delegitimizing.[56]

In sum, most objections to malattributed comments rest, implicitly or explicitly, on the misconception that notice-and-comment rulemaking is a referendum.[57] For that reason, they are misplaced.

IV. SO WHAT IS THE HARM FROM MALATTRIBUTED COMMENTS?

The previous Section argued that viewing malattributed comments as per se problematic or delegitimizing rests on a category mistake. Once comments are understood as inputs in a deliberative, reasoned process rather than a vote, the problem becomes more dilute and harder to

---

56 In the words of one long-time, highly respected Department of Transportation attorney, Neil Eisner, who was defending anonymous rather than pseudonymous comments, a "comment should be judged on its merits rather than the name [of the submitter]. If anonymous, I may not give it the same consideration as I would to a known expert, but if they are correct in their point and provide proof that our proposal would cause harm," it should not be ignored just because it is anonymous. Comment of Neil Eisner, AUCS Committee on Regulation (April 25, 2011), https://www.acus.gov/sites/default/files/documents/COR-2d-Mtg-Eisner-Comment.pdf [https://perma.cc/5BDN-LS4C].

57 *See, e.g.*, Karl Bode, *The FCC Insists it Can't Stop Impostors From Lying About My Views On Net Neutrality*, TECHDIRT (July 11, 2017, 3:23 AM), https://www.techdirt.com/articles/20170710/10071737756/fcc-insists-it-cant-stop-impostors-lying-about-my-views-net-neutrality.shtml [https://perma.cc/AS3F-B8D7] (expressing dismay that the FCC is "doing nothing about the pile of bogus comments (some of which originate from dead people) spoiling what should be a simple democratic exercise"); *id.* (comment of "Anonymous Coward" July 11, 2017 4:21 PM) ("One person/group of people using others' identity without permission to say something on their behalf is absolutely a violation of the democratic principle as that person is over-representing his/herself.").

identify with particularity. Vague assertions that the process has been "tainted"[58] or "corrupted,"[59] or lacks "integrity,"[60] sound troublesome but are exceedingly imprecise. This Part attempts to pin down the harms. Section A discusses the possibility that such comments lead to bad regulatory outcomes; this would be a serious negative consequence but seems unlikely to happen. The remaining subsections touch on harms that seem more real; though not trivial, they are still rather modest.

One point at the outset. There is nothing good about malattribution. Whatever value a malattributed comment may have as a comment would still exist were it submitted anonymously or under an accurate identity. Thus, there is no benefit to offset whatever harm they cause. They do cause some harm, and accordingly some efforts should be made to control and contain them. But we cannot assess how extensive such efforts should be without a real grasp of the actual harms. Moreover, unless we are very clear-eyed about costs and benefits, efforts to prevent or neutralize these harms may have unintended negative consequences that match or exceed those of inauthentic comments.

A. *Bad Regulatory Outcomes*

The quality of an agency regulation depends on the agency both having the information it needs and not getting misled or distracted by information that is irrelevant or false. Notice-and-comment rulemaking is a deliberative policymaking process where the agency relies on

---

58 Memorandum of Law in Opposition to Defendant's Motion for Summary Judgment and in Support of Plaintiffs' Cross-Motion for Summary Judgment at 5, New York Times Co. v. FCC, No. 1:18-cv-08607-LGS (S.D.N.Y. Apr. 10, 2019), 2019 WL 3991285 (stating that "the public comment process in the net neutrality rulemaking was tainted by fraud").

59 Brian Fung, *FCC Net Neutrality Process 'Corrupted' by Fake Comments and Vanishing Consumer Complaints, Officials Say*, WASH. POST (Nov. 24, 2017, 1:28 PM), https://www.washingtonpost.com/news/the-switch/wp/2017/11/24/fcc-net-neutrality-process-corrupted-by-fake-comments-and-vanishing-consumer-complaints-officials-say [https://perma.cc/STV5-FZB7].

60 Cheryl Bolen, *Are You Real? U.S. Hunts Fakers Among 10,000 Commenters on Rules*, BLOOMBERG GOV'T (June 20, 2019, 12:00 AM), https://about.bgov.com/news/are-you-real-u-s-hunts-fakers-among-10000-commenters-on-rules [https://perma.cc/9U4J-E7HG] ("While agencies take any fraud seriously, public comments aren't the equivalent of votes for a rule, so the effect of comments with false identities on a regulation is minimal. Still, Democratic lawmakers say any use of false identities can taint the integrity of rulemaking.").

commenters to provide information. If the agency is misled or misinformed, the result will be a suboptimal regulation. The question is whether malattributed comments pose a significant risk of having such destructive influence.[61] The series of *Wall Street Journal* articles highlighting the net neutrality fiasco was entitled *Hidden Influence*.[62] That certainly flags the core concern—phony comments are influencing policy, and policy based on falsehoods is bound to be bad policy. Well, are malattributed comments influential? And if so, is the use of false names what makes them so?

The answer should be no. First, if the fear is that the agency will misapprehend the level of support for one position or another,[63] that error (a) is not relevant, as discussed above, (b) for that reason is unlikely to affect the agency decision even if it did mislead, because the agency should not, and generally is not, interested in counting heads, (c) has nothing to do with the use of other people's names; the same result could occur with a raft of computer-generated anonymous filings, and (d) is unlikely to happen at all, since agencies will be unlikely to view comments as meaningful indicators of the level of public support.

---

61 In arguing for the release under the Freedom of Information Act (FOIA) of information regarding the source of computer-generated malattributed comments, the *New York Times* took exactly this view of the harm from malattributed comments:

> The public interest in getting and analyzing the contents of the API proxy server logs is considerable. Among other things, the logs will likely reveal the true extent of the fraud that infected the net neutrality rulemaking, including the extent to which cloud-based automated bots intervened in an important public debate. In the wake of Special Counsel's Robert Mueller's recent indictment of 13 Russian individuals and three Russian companies for interfering with U.S. elections and the U.S. political system, the public interest in understanding how these cloud-based automated bots are being used to influence an array of U.S. political activities—including the agency notice-and-comment process—is exceptionally high . . . Put simply, the data can tell us who corrupted the notice-and comment process, and how they did it.

Memorandum of Law in Opposition to Defendant's Motion for Summary Judgment and in Support of Plaintiffs' Cross-Motion for Summary Judgment, *supra* note 58, at 16; *see also* Prechtel v. FCC, 330 F. Supp.3d 320, 331 (D.D.C. 2018) (stressing public interest in clarifying whether "the Commission succeeded—as it assured the American people it had—in managing a public-commenting process seemingly corrupted by dubious comments").

62 *See* Grimaldi & Overburg, *supra* note 7.

63 *See, e.g.*, Katherine Krems, *Crowdsourcing, Kind Of*, 71 FED. COMM. L.J. 63, 76 (2018) ("[T]he FCC will not be able to properly gauge public sentiment without a record that actually reflects public sentiment.").

Ultimately, this is an empirical question; it is not enough to say that the answer "should be" no. To my knowledge, no one has done the necessary work to determine whether mass, bot-generated, or malattributed comments have been influential. My sense is that they are not at the career level. Career rule-writers view their broad job as developing sound policy and their narrow job as responding to substantively important comments. Comments that do not require a response are ignored. But that may not be true of political appointees, who may be looking for confirmation or selling points. Political appointees, and the White House, care about public approval and how a proposal plays. They may be nervous about a large-scale negative response and reassured and emboldened by large-scale support. They also may be less focused on technical details, the quality of supporting data, and legal constraints that preoccupy career rule writers, which leaves more room for vote counting.

Nonetheless, the risk here seems relatively low. The most likely scenario is that an agency will latch on to apparent but bogus support to justify something it would do anyway; it is an ex post justification but not an actual cause of the decision. Moreover, if this occurs, it is not a problem with malattributed comments per se; it is a problem with any computer-generated comments and indeed any comments submitted pursuant to an organized campaign. Also, even if the comments are influential the ultimate decision must still be justified as reasoned decision-making; the agency rule will be set aside if all the agency can say in its defense is that lots of commenters were supportive. Finally, just the opposite phenomenon is also possible. That is, the agency may react negatively to being swamped by repetitive submissions of dubious pedigree and, as a result, discount the comments and move away from the position they advocate. There is some empirical support for this supposition.[64]

Second, mass and malattributed comments tend to contain very little information, generally repeating what a known person has said or stating a bottom-line preference for a particular outcome. Thus, there is nothing in the typical malattributed comment that will be influential. One thing that in most circumstances will *not* be influential is the use of a

---

64 Stuart W. Shulman, *The Internet Still Might (But Probably Won't) Change Everything*, 1 ISJLP 111, 138–39 (2005).

random person's name and address, whether that person is the actual sender of the comment or not.

Third, *someone* believes the comment, that is why it is being submitted. It is a real comment, submitted by someone who wants the agency to act in accordance with the comment. So its *content* is not the problem. To the extent it says something of substance, there is no reason not to consider what it says. Put differently, not only will the comment likely not have any influence, any influence it does have is unlikely to be untoward.

Focus on malattribution in particular. That is a false piece of information being communicated to the agency. Is it a cause for concern in the sense that it might affect the outcome for the worse? It is hard to see how.

Use of false names on duplicative comments is potentially misleading in two possible ways. First, it is possible that a single entity or person submits multiple comments under multiple names. There is only one entity or person behind the multiple comments, but it looks like there are many. So what is misleading is not the content of the comments but their apparent number. If numbers count, that could be important. If numbers are irrelevant, then this is just not misleading in a relevant, meaningful, or, to use the legal term, material way.

Second, the names themselves are false and therefore potentially misleading. Not very, though. The malattributions that often grab observers' attention involve using the name of a famous (sometimes dead) person. But these are not misleading; anyone would realize that the name is false. For example, in the net neutrality rulemaking, there were multiple submissions from "Barack Obama" and from "Ajit Pai."[65] This is not deceptive; no rulemaking official would think that the former President or the FCC Chair had submitted the comment. Ditto for submissions from "Elvis Presley."

Even if the phony name is not a household name but a big shot in the relevant field—say a professor, consultant, or lobbyist—it is highly

---

[65] *See, e.g.*, "Barack Obama," ID 1051157755251, FCC Proceeding 17-108 (May 11, 2017), https://ww.fcc.gov/ecfs/filing/1051157755251 [https://perma.cc/8DVS-QESE] (submission from "Barack Obama" of "1600 Pennsylvania Avenue, Washington, DC," objecting to the "unprecedented regulatory power the Obama Administration imposed on the internet" and "Obama's . . . power grab").

unlikely that the ruse would work. If the name is on one of among thousands of duplicative comments, it likely will not even be noticed. If it is noticed, the effect will be minimal because even experts do not influence rule writers by merely expressing an outcome preference. On the other hand, if the comment is unique and substantive the name will be noticed but the deception will likely be apparent. If it is not, the potential problem is not with the false name but with false content (if any). This question of unreliable content exists wholly separate from the malattribution phenomenon, and the agency always has some obligation to double-check information and data on which it is actually relying. And, last, if the name given is unknown, then it is not misleading because the name carries no significance. The submitter's name in itself does not go to the *weight* of the comment. The comment is not more powerful if signed by David Jones, whoever that is, than if it is signed by William Smith, whoever *that* is.

To illustrate the foregoing, consider the comment from an individual set out in the footnote.[66] This was submitted in a Federal

---

[66] I am writing to endorse the comments submitted to Docket # FHWA-2013-0020 by the League of American Bicyclists.

I believe that performance measures on our transportation system should include measures that reflect all users—including bicyclists and pedestrians. Specifically I'd like to comment on three of the performance measures in this rule.

National Highway System (NHS) Performance

In the FAST Act, Congress made clear that states must consider all modes and users in the building and reconstruction of NHS projects. However, this rule proposes to measure reliability of the system by travel time for motor vehicles ONLY.

The reliability of the NHS must include a measure for ALL users. For bicyclists and pedestrians reliability should be measured by safe access on NHS roads.

Congestion Mitigation

The rule proposes that congestion mitigation be measured by delay for drivers. It fails to measure people not adding to that congestion because they are biking, walking or taking transit.

Many states and metropolitan areas have goals to reduce congestion by reducing vehicle miles traveled and/or to increase mode share for bicycling, walking and transit use. To make this rule more compatible with these goals, a new measure should be added to account for people traveling by modes that reduce congestion: transit, bicycling and walking.

Mobile Source Emissions

Highway Administration rulemaking regarding standards for measuring state progress toward achieving federal transportation goals. It is intelligent, substantive, and informed, if somewhat unelaborated and stronger on the what than the how or the why. The issues raised would merit a discussion in the preamble to the final rule (and received it).[67]. But there are two characteristics of this comment that might be relevant to its evaluation and consideration. First, it is one of 5,858 *identical* comments (out of about 8,000 total comments). Evidently it was drafted by the League of American Bicyclists, 6,000 of whose members submitted the suggested text or something almost identical to it. How 6,000 identical comments differ from a single comment with the same text, if at all, is the issue of mass comments, outside the scope of this article.

Second, this particular comment was submitted by Elvis Presley.[68] How to explain that? One possibility is that The King is in fact still alive and—who knew?—really interested in promoting bicycling. Possible, but unlikely. Another is that somewhere in America there is a person who has that name but is not *the* Elvis Presley, and he is very interested in promoting bicycling. And the third is that someone not named Elvis Presley, but interested in promoting bicycling, wanted to comment without giving his name and so used a pseudonym. The point is that *it does not matter which of these three things is true*. The value of the comment depends entirely on its content, not the "from" line of the email.

What might affect the weight of the comment is the biography of the commenter. Is it someone with particular expertise? With "situated

---

> I support the inclusion of greenhouse gas emissions both from tailpipes and from construction of new projects. The transportation system is responsible for 23 percent of the country's emissions, and in order to meet the goals and commitments made at the Paris COP we need to start measuring and reducing emissions.
>
> I appreciate the opportunity to comment on the rule, and support the move to a performance-based transportation system.
>
> I hope the final performance measures will reflect the Secretary's leadership to serve all users of the transportation system.

67 Federal Highway Administration, National Performance Management Measures, 82 Fed. Reg. 5970, 5981 (Feb. 17, 2017).

68 Federal Highway Administration, National Performance Management Measures, Docket #FHWA-2013-0054, Comment from Elvis Presley (posted Aug. 29, 2016), https://www.regulations.gov/document? D=FHWA-2013-0054-6039 [https://perma.cc/V7UY-YSA2].

knowledge"?[69] Who has done relevant research or had direct personal experience? Who will be directly regulated or affected? All those people possess information that members of the general public do not and that the agency should know. They may also have a stake that should counsel caution in taking their assertions at face value. For both reasons, it is useful to know who the source of the comment is. But biographical misrepresentations are part of a larger and distinct problem not specific to "fraudulent" comments, that of the accuracy, completeness, or representativeness of assertions within comments. If an agency relies on crummy information, it will write crummy rules. At best, crummy information in comments is a distraction, requiring time and effort to debunk before being ignored. However, the system works pretty well to deal with that problem. Agencies have expertise. They receive other comments.[70] And at least so far, malattributed comments are not crammed with false information because they are not crammed with information, full stop.

B. *Distraction and Inefficiency*

A frequent assertion is that malattributed comments overwhelm the system, distract agency attention, and can "shut out" other legitimate voices that should be heard. FCC Commissioner Rosenworcel has made this point repeatedly with regard to the net neutrality rulemaking. In her view, "the public is increasingly shut out of decision-making by the fraud that is flooding public channels for comment."[71] Others have made the same argument.[72] It is not exactly clear what the mechanism of shutting

---

69 *See* Cynthia R. Farina, Dmitry Epstein, Josiah Heidt, & Mary J. Newhart, *Knowledge in the People: Rethinking "Value" in Public Rulemaking Participation*, 47 WAKE FOREST L. REV. 1185, 1187–88, 1197 (2012) (describing "situated knowledge" as "information about impacts, ambiguities and gaps, enforceability, contributory causes, unintended consequences, etc. that is known by participants because of their lived experience in the complex reality into which the proposed regulation would be introduced").

70 I suggest in Part VI below that one response to the problem of fraudulent comments would be greater use of reply periods so as to crowdsource the scrutiny of submissions for information quality problems.

71 Rosenworcel, *supra* note 44.

72 *See, e.g.*, Krems, *supra* note 63, at 76 (noting that "false information . . . overshadows real public comments that reflect public sentiment" and "illegitimate comments minimize the impact

out is and Commissioner Rosenworcel does not provide details. She is on the inside, and perhaps we should take her word for it. But there is reason to be skeptical.

First, to the extent the volume of comments is a problem, it is not a *malattributed comments* problem. Rather, it is what Livermore, Eidelman, and Grom call a "haystack problem."[73] "The haystack problem occurs when comments of high substantive value are hidden within a very large set of documents of lower substantive value, creating the risk that agencies will fail to locate and appropriately consider high-value comments."[74] If a million people submit the same comment pursuant to a mass comment campaign, deduplication software can easily identify them and avoid swamping readers. But if a million people submit unique comments, or if a bot produces a million comments that are sufficiently distinct to get past the deduplication software, then readers will be swamped.[75] Yet that problem is not the result of, and exists in the absence of, the use of phony identities. It will arise whether the comments have false names attached to them or not.[76]

In any event, concerns over real voices being drowned out misunderstands the nature and goals of the notice-and-comment process. The misconception is common and fostered in part by government agencies themselves. But misconception it is. The mistake is in thinking that the point of the comment process is to "let every voice be heard."[77]

---

of those that are legitimate"); *id.* at 82 (noting that "when fake comments dominate, legitimate comments may be overlooked").

73 Michael A. Livermore, Vladimir Eidelman & Brian Grom, *Computationally Assisted Regulatory Participation*, 93 NOTRE DAME L. REV. 977, 1016–17 (2018).

74 *Id.* at 981.

75 Bridget C.E. Dooling, *Legal Issues in E-Rulemaking*, 63 ADMIN. L. REV. 893, 899–901 (2011).

76 For a useful discussion of technical responses to the haystack problem and its counterpart, the "forest problem," i.e. the challenge of getting an overall perspective on the totality of comments, see Livermore et al., *supra* note 73.

77 The front page of regulations.gov includes the subtitle "Your Voice in Federal Decisionmaking" and invites users to "Make a Difference. Submit your comments and let your voice be heard." *Make a difference. Submit your Comments and let your Voice be Heard*, REGULATIONS.GOV, http://www.regulations.gov [https://perma.cc/2SBN-C3XD]. Similarly, when regulations.gov held a competition for short videos to promote the site, the winning submission promises that the Internet makes it easier than ever to "let your voice be heard" and concludes with three ordinary citizens each admonishing the viewer to "let your voice be heard."

One problem with conceiving this as the goal is that it is self-defeating. The more successful agencies are in getting individuals to submit comments in broadly consequential or controversial rulemakings, the less any individual submitter's "voice" will get through. This is a universal truth about the Internet—everyone can speak, which means it is very hard to be heard. As the editor-in-chief of the *Huffington Post* observed in explaining the decision to shut down the publication's longstanding platform for unpaid, "citizen journalists," unfiltered platforms devolve into "cacophonous, messy, hard-to-hear places where voices get drowned out and where the loudest shouting voice prevails."[78]

More importantly, the goal is not to hear individual voices. Rather, it is to ensure that the agency is fully informed. Repetitive comments are not helpful; empty statements of a bottom-line are not helpful. Suppose the Fish and Wildlife Service proposes to list a species as endangered. Say (unrealistically) that it only gets one hundred comments. No problem of swamping or drowning out here. Fifty of the comments are from experts of one sort or another; fifty are from lay-persons who express a clear view—some pro, some con—regarding the listing but do not include any information or argument. When the final rule comes out, the preamble will not mention or respond to those latter fifty comments because they included nothing to respond to. Were the "voices" of those fifty "heard"? Literally, yes. But they made no contribution to the rulemaking and had no effect on its outcome. This was not because they were drowned out.

Ignoring empty and/or duplicative comments is not nefarious, though it is sometimes perceived that way. The government analytics firm FiscalNote has studied FCC rulemaking notices and created what it calls a "gravitas score" to predict how much attention a comment will get from the agency. Reportedly, it "found that often, only comments that include a serious legal argument or are affiliated with some known entity like a big business or academic institution, make their way in" to the

---

Timothy Ide, *The Rulemaking Matters! Mosaic*, YOUTUBE (May 17, 2010) http://www.youtube.com/watch?v=hRXFcurpE7U [https://perma.cc/RNN9-TEM2].

78 Sydney Ember, *HuffPost, Breaking From Its Roots, Ends Unpaid Contributions*, N.Y. TIMES (Jan. 18, 2018), https://www.nytimes.com/2018/01/18/business/media/huffpost-unpaid-contributors.html [https://perma.cc/X5TG-JL9C] (quoting Lydia Polgreen).

preamble of the final rule.[79] The implication is that the agency pays attention only to big shots. But, of course, the mere fact that comments from "a big business or academic institution" earn replies does not prove that it is the identity of the commenter that is the causal explanation. It seems more likely that the identity of the commenter and the preambular response are both related to a third, important, and legitimate factor: the substance of the comment.[80]

A slight variation on this objection posits that agencies will ignore malattributed comments because of their source and in the process *also* ignore authentic ones, throwing the baby out with the bathwater. It is not clear why this should happen. If the agency segregates malattributed comments, it will not (and that is an argument for making some effort to do so). Even without such a process, the baby goes out with the bathwater only if the agency is just counting heads and concludes that since so many votes are fake the overall vote tally cannot be trusted. At this point, the reader knows the response to that objection and I will not repeat it.

For all these reasons, the "swamping" or "drowning out" hypothesis is unconvincing. The most that can be said is that any deluge of unique comments, malattributed or not, must slow things up somewhat, with little or no offsetting benefit.

C. *Loss of Public Confidence*

News coverage of the malattributed comments issue surely has had some impact on public confidence in the integrity and legitimacy of agency rulemaking. I am not aware of any actual polling on this, but casual attention to social media tends to confirm what one would suspect anyway. Neither the amount of the decline, nor the harm it causes, can be quantified. But at a time when trust in government is otherwise

---

79 Issie Lapowsky, *How Bots Broke the FCC's Comment System*, WIRED (Nov. 28, 2017, 12:19 PM), https://www.wired.com/story/bots-broke-fcc-public-comment-system/ [https://perma.cc/9TZ3-7KS2].

80 Mariano-Florentino Cuéllar, *Rethinking Regulatory Democracy*, 57 ADMIN. L. REV. 411, 430 (2005) (concluding that "sophistication," i.e. "rhetorical, cognitive, and technical complexity," not commenter identity, predicts whether an agency adopts a comment's suggestions).

extraordinarily low, this phenomenon has only further corroded public confidence.

It is important to recognize, however, that the real villain here is not malattributed comments but rather civic ignorance: the faulty assumption, on the part not only of ordinary citizens but also of media and other opinion leaders, that rulemaking is like elections and comments are like votes. To the extent malattributed comments undermine public confidence the problem could indeed be cured by eliminating the comments, but it could also be cured by public education regarding the nature of the comment process.

D. *Harm to "Identity Theft Victims"*

One group, or at least some members of one group, feels a particular and personal harm from malattributed comments: those whose names were attached to comments they did not submit. As I discuss below, I do not think it appropriate, legally or in lay terms, to call this "identity theft," though many do. And while there are identifiable human victims, the harm is rather dilute and abstract. If I had the choice between, on the one hand, having someone submit a comment with which I disagreed under my name and with my email address and, on the other, having that person clean out my bank account, I would certainly go with option one. In Thomas Jefferson's words, a malattributed comment "neither picks my pocket nor breaks my leg."[81] However, it has not happened to me. Some of those to whom it has happened are very upset.[82] They feel a real sense

---

81 THOMAS JEFFERSON, NOTES ON THE STATE OF VIRGINIA 169 (1788) ("The legitimate powers of government extend to such acts only as are injurious to others. But it does me no injury for my neighbour to say there are twenty gods, or no god. It neither picks my pocket nor breaks my leg.").

82 *See, e.g.*, *Thousands of Fake Comments on Net Neutrality: A WSJ Investigation*, *supra* note 10 (describing reaction of one "horrified" person whose name had been used). A group letter from 27 individuals—not such a huge number, given the denominator—whose names were used to file malattributed comments with the FCC communicates a sense of having been wronged. *See Letter to the FCC from People Whose Names and Addresses Were Used to Submit Fake Comments Against Net Neutrality*, FIGHT FOR THE FUTURE (May 25, 2017, 10:40 AM) https://www.fightforthefuture.org/news/2017-05-25-letter-to-the-fcc-from-people-whose-names-and [https://perma.cc/4EPC-STMB].

of violation, intrusion, and expropriation, even if it is a little difficult to pin down the exact harm that has occurred.[83]

One can imagine a more substantial individual harm. In a world in which a single ill-considered tweet can destroy reputations and careers, severe reputational harm can flow from holding a repellent position. If the position is one that the person does not in fact hold, the harm is that much more severe. Suppose, for example, the Interior Department were to hold notice-and-comment proceedings on President Trump's proposal to create a "National Garden of American Heroes,"[84] and a troll farm submitted public comments, under real people's names, that advocated for the inclusion of Confederate generals and the exclusion of Black heroes. Now suppose that, given the salience of the issues and the boldness of the comments, the comments were discovered by the media, prospective employers, or just a few people with large twitter followings.[85] Denying, truthfully, that you actually submitted the comment is unlikely to solve the problem. Given how invisible rulemaking dockets are, this scenario is unlikely. It requires a particular confluence of circumstances. And as online threats to reputation go, it is pretty far down the list. But it is not inconceivable.

E. *Cover for an Agency Operating in Bad Faith*

Thus far I have been assuming, perhaps naïvely, that the agency is acting in good faith. That will not always be the case, unfortunately. An agency official pursuing a predetermined outcome and looking for cover may find it in malattributed comments. The FCC rulemaking is not an example; if the FCC was operating in bad faith it was in that it had its mind made up before the comment period. There is no indication that it was influenced by, relied on, overemphasized, or trumpeted the

---

83 One hint as to the challenge of pinning down the exact harm is the vagueness of a statement from the California Department of Justice that "urge[d] Californians to check whether they have been impacted" by the malattributed comments in the net neutrality proceeding. Kevin Oliver, *More Sacramento Victims Discovered in FCC Fake Comments Scam*, KCRA (Dec. 15, 2017), http://www.kcra.com/article/more-sacramento-victims-discovered-in-fcc-fake-comments-scam/14445643 [https://perma.cc/8LRP-KK68]. How would Californians actually go about "checking" for "impact"?

84 *See* Exec. Order No. 13934, 85 Fed. Reg. 41,165 (July 3, 2020).

85 I am indebted to Jonathan Rusch for the hypothetical.

malattributed comments. But a pending SEC rulemaking provides a cautionary tale. In December 2019, the SEC proposed a rule regarding exemptions from the proxy rules for proxy voting advice.[86] Prior to the proposal, it held a roundtable in 2018 and invited follow-up submissions, of which it received about five hundred. In announcing the proposed rule, the Commission Chair, Jay Clayton, invoked several of these:

> Some of the letters that struck me the most came from long-term Main Street investors, including an Army veteran and a Marine veteran, a police officer, a retired teacher, a public servant, a single Mom, a couple of retirees who saved for retirement, all of whom expressed concerns about the current proxy process.[87]

Later reporting put those letters in a different light. All had been assembled, organized, and written by an industry group called the 60 Plus Association, which is funded by supporters of the SEC proposal.[88] The retired teacher did sign her letter but had not written it; the vets were the brother and cousin of the chair of 60 Plus; the single mom did not write her letter; the retired couple were the in-laws of the head of 60 Plus and when contacted had no recollection of ever writing any such letter; the public servant reported that she had been contacted by a public affairs firm out of the blue, that she did not know what a proxy adviser is, and "[t]hey wrote [the letter], and I allowed them to use my name after I read it. I didn't go digging into all of this."[89]

Clayton has been evasive when questioned about the letters, insisting, as one would expect, that the proposed rule will protect "Main Street investors" even if the specific Main Street investors he invoked

---

86 *See* 84 Fed. Reg. 66518 (proposed Dec. 4, 2019) (to be codified at 17 C.F.R. 240).

87 Statement of Jay Clayton, SEC Chairman, at Open Meeting on Proposals to Enhance the Accuracy, Transparency and Effectiveness of Our Proxy Voting System (Nov. 5, 2019), https://www.sec.gov/news/public-statement/statement-clayton-2019-11-05-open-meeting [https://perma.cc/EV3H-ZRA2].

88 Zachary Mider & Ben Elgin, *SEC Chairman Cites Fishy Letters in Support of Policy Change*, BLOOMBERG (Nov. 19, 2019, 10:03 AM), https://www.bloomberg.com/news/articles/2019-11-19/sec-chairman-cites-fishy-letters-in-support-of-policy-change [https://perma.cc/ER4B-NZ7P].

89 *Id.* All in all, 60 Plus got about two-dozen people with connections to the organization to submit letters. The 60 Plus president insisted, by the way, that his mother- and father-in-law *had* known about the letter they supposedly submitted: "They are 80-some-years-old. This happened months ago. I'm sure it's not top of their minds." *Id.*

were actually a front for a corporate lobbyist.[90] Did these letters actually have an impact on the SEC? It is possible, but it seems more likely that they were useful material to cite in support, as the folks at 60 Plus knew they would be. Clayton did not want to be seen as the tool of large corporate interests. Invoking the manufactured letters was more public relations than "reasoned decision-making." But the real failing was not that the letters had such a dubious pedigree but that Clayton was making policy based on snippets and anecdotes, like Presidents of both parties do when pointing to invited guests at the State of the Union address.[91]

In any event, this little episode (itself only an anecdote that should not be too heavily relied upon) is not a cautionary tale about standard "fraudulent comments." None or almost none of the letters were submitted in the name of someone who did not know about it. Rather, it is a cautionary tale about inaccuracy. The *content* of the letters was misleading; for the most part the *names* of the submitters were not. Again, that is always a potential problem, to which the agency must be alert, but one that is distinct from the problem of malattributed comments at issue here.

V. ARE MALATTRIBUTED COMMENTS ILLEGAL?

Many have asserted that submitting malattributed comments is illegal if not actually criminal. FCC Commissioner Rosenworcel, for example, describes the net neutrality fiasco thus: "As many as nine and a half million people had their identities stolen and used to file fake

---

90 *Oversight of the Securities and Exchange Commission, Hearing Before the Senate Committee on Banking, Housing, and Urban Affairs*, 116th Cong. (Dec. 10, 2019) (testimony of Jay Clayton), https://www.banking.senate.gov/hearings/oversight-of-the-securities-and-exchange-commission [https://perma.cc/WM8C-EN95]. At this hearing, Clayton was pressed by Senator Smith, *id.* at 1:17:10, and berated by Senator Van Hollen, *id.* at 1:49:30. The latter's go-to phrase, used three times, was: "You got duped." *Id.*

91 In fairness, when it appeared, the preamble to the proposed rule did not take this anecdotal approach or mention the misleading letters. *See* 84 Fed. Reg. 66518 (proposed Dec. 4, 2019) (to be codified at 17 C.F.R. 240). Of course, a preamble is written by career staff, not the Commissioners. The gap between Chairman Clayton's public statements and the preamble may indicate that political appointees are more vulnerable to being misled by misattributed or other inaccurate comments. *See supra* at 119. Or it may reflect a rhetorical difference resulting from the different audiences—most importantly, the fact that a key audience for the preamble is a reviewing court.

comments, which is a crime under both federal and state laws."[92] Alas, she does not state what those federal and state laws are. She has lots of company, both in asserting that a crime has been committed and in failing to specify what the crime actually is.[93] This Section reviews possible legal theories.

One observation at the outset. Despite heated rhetoric, it is notable that not one state or federal prosecutor has brought a prosecution arising out of the net neutrality rulemaking or any other instance of so-called fraudulent comments. It is possible, of course, that they just have bigger fish to fry. But the very fact that no prosecutions have been brought in itself at least suggests that the nation's law enforcers have concluded that the activity, however annoying or reprehensible, is not actually criminal or, even if technically so, not sufficiently serious to warrant prosecution.

A. *Fraud*

The most obvious crime that might be committed by filing "fraudulent comments" would be, natch, fraud. The fit is poor.

---

92 *In the Matters of Nicholas Confessore and Jeremy Singer-Vine*, FOIA Control No. 2017-764; FOIA Control No. 2018-204, slip op. at 14 (Dec. 3, 2018) (dissenting statement of Comm'r Jessica Rosenworcel).

93 For example, consider this exchange between *National Public Radio*'s Ari Shapiro and *Wall Street Journal* reporter James Grimaldi:

> SHAPIRO: I mean, do you generally see the same language over and over again? Do you see made-up names? Do you see names of dead people?
>
> GRIMALDI: Yeah. Well, all of the above. We found a lot of that. But the thing we were most interested in beyond the fake names who are Barack Obama when we knew it wasn't him, we were looking for people whose identities appear to have been stolen or used in some way or tricked to put a comment that they didn't agree with.
>
> SHAPIRO: This is actually a felony. Is there any accountability here?
>
> GRIMALDI: So far, there's really no enforcement of this rule.

"WSJ" Analysis Shows Fake Comments Submitted to Government Agencies, ALL THINGS CONSIDERED (Dec. 27, 2017), https://www.npr.org/2017/12/27/573870693/wsj-analysis-shows-fake-comments-submitted-to-government-agencies [https://perma.cc/B4BY-GV35].

1. General Principles

Fraud and misrepresentation are not the same thing. A flat lie about the commenter's identity involves a misrepresentation, but a misrepresentation is only one part of the crime or tort of fraud. The classic statement of common-law fraud—"five finger fraud"—has five elements: (1) a false statement of a material fact, (2) knowledge on the part of the defendant that the statement is untrue, (3) intent on the part of the defendant to deceive the alleged victim, (4) justifiable reliance by the alleged victim on the statement, and (5) injury to the alleged victim as a result.[94] The injury must involve the deprivation of money, property, or a legal right.

Some of these requirements are undeniably met by malattributed comments. They do involve a false statement of fact. (Whether that false statement is *material* is a separate question that I put aside until Section 2.e, below.) The maker of the statement surely knows that the statement is untrue. Often, there will be an intent to deceive, though when a comment is submitted under the name of the agency head, or Mickey Mouse, or Barack Obama, or Elvis Presley, the impossibility of actual deception negates intent. But the final two requirements are very problematic. It will be rare that the agency relies on the stated identity of the commenter. If the comment is duplicative—as is generally the case—most agencies will not even read the duplicates and so not even notice, let alone rely on, the name of the persons allegedly submitting. Further, if it has not relied on and is unaware, then by definition the fifth prong is not satisfied because any injury is not "as a result" of the false statement.

But assume that somehow or other the agency does rely on the fact that a comment purports to be from a particular individual when it is not. How might this harm the agency? It would do so only if the agency places particular weight on, or heavily discounts, the comment in light of the identity of the person who supposedly wrote it. An agency might do that when the comment comes from a very well-known or well-placed source. The Department of Transportation (DOT) will pay particular attention to comments from General Motors (GM) or Ralph Nader when

94 *See, e.g.*, Cornelison v. TIG Ins., 376 P.3d 1255, 1270 (Alaska 2016); Commonwealth v. Lucas, 34 N.E.3d 1242, 1249 (Mass. 2015); Pasternack v. Lab. Corp. of Am. Holdings, 59 N.E.3d 485, 491 (N.Y. 2016).

establishing vehicle safety standards. But it is hard to imagine a malicious commenter successfully convincing DOT that she is actually GM, particularly if the real GM has a sufficient interest in the proceeding to file a comment or at least monitor the docket. Thus, it is unlikely that there is an actual harm to the agency.

Moreover, if there is a harm, it will be that it reached a policy conclusion that it would not otherwise have reached. This may be conceptualized as a harm to the agency or as a harm to either the regulated community or to regulatory beneficiaries (depending on the direction of the error). One problem with the second conceptualization is that courts are reluctant to allow a plaintiff (here a regulated entity or regulatory beneficiary) to establish the reliance element of a fraud claim by showing that a third party (here the agency) relied on the defendant's false statement.[95] Furthermore, it is not at all clear that "bad policy" is the sort of injury that qualifies under the fifth prong. The cases are replete with statements that the requisite injury must be "of a pecuniary or substantial character."[96] The boundaries are debatable, of course, but we are certainly some distance from the classic setting involving a specific and tangible physical loss.[97]

Finally, and most importantly, the causation problems with this claim are overwhelming. Proving that if only the agency had known the actual source of a pseudonymous comment, it would have reached a different outcome, would be impossible. In the net neutrality rulemaking the idea is laughable, and in any setting the causal chain would be obscure at best. It is hard enough to know whether comments as a whole have an influence; harder still to show that a single comment was influential; harder still to show that the false identity attached to a comment was influential; and impossible to show that that "influence" was powerful enough to affect the outcome of the rulemaking.

---

95 *Pasternack*, 59 N.E.3d 485; *but see* Bridge v. Phoenix Bond & Indem. Co., 553 U.S. 639, 653 (2008).

96 37 C.J.S. *Fraud* § 69 (2020).

97 The following subsection returns to this issue under federal law.

2. Federal Fraud Crimes

The federal criminal code includes a variety of fraud crimes. Much of the foregoing discussion applies to possible prosecutions under those provisions, but a few specific comments are in order.

a. Mail Fraud and Wire Fraud

The basic and oldest federal fraud provision outlaws the use of the mail as part of "any scheme or artifice to defraud."[98] The wire fraud provision uses similar language.[99] Any comment that is not hand-delivered is communicated either by mail or by computer; if the latter, a "wire" is used. Accordingly, one or the other of these provisions applies to the submission of almost all rulemaking comments. Is misleading an agency as to the identity of a commenter criminal fraud?

The crime requires a "scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises."[100] This could be read to reach two different kinds of conduct: (a) a scheme to defraud or (b) a scheme to obtain money or property through false or fraudulent statements. So read, the "scheme to defraud" would be illegal even if not part of an effort to obtain "money or property." However, courts have uniformly "[c]onstru[ed] that disjunctive language as a unitary whole," so the "money-or-property" requirement applies equally across the board.[101] The property can be *intangible*—information, a right to collect payment in the future—but must still be something historically understood as a property interest.[102]

---

98 18 U.S.C. § 1341 (2018) (making it a crime to use the mails "for the purpose of executing" or attempting to execute a "scheme to defraud, or for means of obtaining money or property by means of false or fraudulent pretenses, representations, or promises").

99 *Id.* § 1343.

100 *Id.* § 1341 (2018).

101 Kelly v. United States, 140 S. Ct. 1565, 1571 (2020).

102 Pasquantino v. United States, 544 U.S. 349, 355–56 (2005) (holding that Canadian government's entitlement to uncollected taxes on liquor imported by the defendant constituted "property"); Carpenter v. United States, 484 U.S. 19, 25–26 (1987) (applying the statute to a scheme to obtain confidential business information); United States v. Hedaithy, 392 F.3d 580, 590 (3d Cir. 2004) "("[T]he object of the alleged scheme or artifice to defraud must be a traditionally recognized property right."); Lombardo v. United States, 865 F.2d 155, 159–60 (7th

In addition, conviction requires establishing specific intent to defraud. An intent to make a false statement is deceit but not fraud; the defendant "must specifically intend to lie or cheat or misrepresent with the design of depriving the victim of something of value."[103] And, again, that "something of value" must be money or property. It is very hard to fit an effort to influence policy outcomes in rulemaking into this box.

In *McNally v. United States*,[104] the Supreme Court relied on this definition of "defraud" in reversing a conviction resting on the intangible deprivation of public employees' "honest services."[105] Congress quickly amended the definition of "scheme to defraud" to include deprivation of the "intangible right of honest services."[106] That vague phrase sowed decades of confusion, as courts searched for principled boundaries to the conduct constituting a deprivation of this "intangible right."[107] The uncertainty culminated in the Court's 2010 decision in *Skilling v. United States*.[108] Motivated in part by concerns over notice and vagueness, the Court held that the deprivation of honest services extends *only* to instances of bribes and kickbacks.

Applying the mail and wire fraud provisions to submission of "fraudulent comments" requires a showing that the submitter had the specific intent either to deprive others of their right to the agency's "honest services" or to obtain money or property. *Skilling* precludes the first theory; there is nothing resembling a bribe or kickback here. The second theory is initially more plausible. Many submitters are likely financially motivated. Certainly hackers or public relations firms retained to do the actual work of creating and submitting the comments are doing it for the money. The underlying motivation for whoever is in the background may be ideological or disruptive, but presumably many or most seek a policy that will be in their economic interest. Even if this chain of causation leading to money or property suffices, however, this

---

Cir. 1989). *Cf.* Cleveland v. United States, 531 U.S. 12, 19–23 (2000) (finding that an unissued state license is not "money or property").

103 United States v. Wynn, 684 F.3d 473, 478 (4th Cir. 2012).

104 483 U.S. 350 (1987).

105 *Id.* at 358.

106 18 U.S.C. § 1346 (2018).

107 *See generally* Sorich v. United States, 555 U.S. 1204 (2009) (Scalia, J., dissenting from denial of certiorari).

108 561 U.S. 358 (2010).

theory hits an insuperable doctrinal obstacle. To violate the statute, the scheme must seek to obtain money or property *from the person defrauded*. That is the long-standing, if usually unarticulated, understanding; it characterizes traditional frauds. Usually, the question does not arise; prosecutors rarely bring cases that do not involve a victim who was both lied to and lost property. But when they have, the courts have explicitly held that the money or property obtained must be that of the person defrauded.[109] Obtaining a regulatory regime that in turn enables an entity to charge high prices or obtain more customers and in that way obtain money does not qualify.

The closest case is *Cleveland v. United States*.[110] This was a racketeering prosecution that alleged underlying acts of mail fraud. The alleged mail fraud was the submission of false information in applications to the state of Louisiana for a license to operate a video poker machine. The applicant was a limited partnership and identified two individuals as the beneficial owners of the partnership; in fact those two had nothing to do with the operation; they were the children of one of the actual partners, that partner had tax and financial issues that might have kept him from obtaining the license. The applications thus were undeniably false—false in just the same way that malattributed comments are. But in a unanimous opinion by Justice Ginsburg, the Supreme Court held that they were not fraudulent because they did not deprive the State of

---

109 The leading decision explicitly so holding is probably *United States v. Walters*, 997 F.2d 1219, 1227 (7th Cir. 1998). The setting is not identical to the submission of malattributed comments in that it involved payments from the victim (universities) to another party (student athletes) rather than to the fraudster (a sports agent who had entered into contracts with student athletes that made them ineligible to receive their scholarships). But the principle articulated applies equally in this setting:

> Not until today have we dealt with a scheme in which the defendants' profits were to come from legitimate transactions in the market, rather than at the expense of the victims. Both the "scheme or artifice to defraud" clause and the "obtaining money or property" clause of § 1343 contemplate a transfer of some kind. Accordingly, following both the language of § 1341 and the implication of *Tanner*, we hold that only a scheme to obtain money or other property from the victim by fraud violates § 1341. A deprivation is a necessary but not a sufficient condition of mail fraud. Losses that occur as byproducts of a deceitful scheme do not satisfy the statutory requirement.

Id. at 1227. The opinion is usefully described and elaborated in Thomas J. Miles, *Dupes and Losers in Mail Fraud*, 77 U. CHI. L. REV. 1111 (2010).

110 Cleveland v. United States, 531 U.S. 12 (2000).

Louisiana of property or money. Rather, "whatever interests Louisiana might be said to have in its video poker licenses, the State's core concern is *regulatory*."[111] The license-holder has a property interest in the license, but the un-issued license is not property held by the state, and that is what matters.[112] And it seems no one even argued that it was enough that the goal of the scheme was to obtain a regulatory determination that would in turn allow the fraudster to obtain money from third parties. "We conclude that § 1341 requires the object of the fraud to be 'property' in the victim's hands and that a Louisiana video poker license in the State's hands is not 'property' under § 1341."[113]

Submission of "fraudulent comments" seeks a different kind of government decision—issuance of an economically valuable regulation rather than of an economically valuable permit. But the principles set out in *Cleveland* are identical. The state has not lost anything that qualifies as "money or property."[114] An ulterior financial goal is irrelevant; what matters is what the defendant is seeking to obtain from the defrauded party. Indeed, if there is any distinction between a permit and a regulation, it would seem that the former is the stronger case for application of a theory of fraud. It is at least a kind of property, it is limited in number, it is valuable only to the specific holder rather than a larger class of entities, it is the basis of a more direct and certain financial gain.

Accordingly, whatever it is, submission of "fraudulent comments" is not "fraud" under federal law.[115]

---

111 *Id.* at 20 (emphasis in original).

112 *Id.* at 15 ("It does not suffice . . . that the object of the fraud may become property in the recipient's hands; for the purposes of the mail fraud statute, the thing obtained must be property in the hands of the victim.").

113 *Id.* at 26–27.

114 For a completely different rulemaking case, one that *does* involve fraud, consider *United States v. Blaszczak*, 947 F.3d 19 (2d Cir. 2019). There the alleged fraud involved obtaining confidential pre-decisional information from a rulemaking agency; armed with this information, the defendant knew regulatory outcomes in advance and traded stocks accordingly. This falls within the statute not because the ultimate goal was to make money or because the rulemaking process was involved, but because what was obtained by deceit *from the agency*—the information—qualifies as property. *Id.* at 30–34.

115 The Supreme Court has read into these statutes a materiality requirement. *See* Neder v. United States, 527 U.S. 1, 1–3 (1999). That, too, would bar a fraud prosecution for submitting misattributed comments, but I defer discussion to Section V.B, *infra*.

b. Email Fraud

Title 18 separately prohibits "[f]raud and related activity in connection with electronic mail."[116] At least some malattributed comments are sent by email, and the provision does make it a crime to "relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients . . . as to the origin of such messages."[117] That might apply here except for the restriction to "commercial" messages. This Section does not define "commercial," but it incorporates by reference the definitions in the CAN-SPAM Act.[118] That legislation in turn defines the term "commercial electronic mail message" as "any electronic mail message the primary propose of which is the commercial advertisement or promotion of a commercial product or service."[119] That is not what malattributed comments are.

c. Computer Fraud and Abuse Act

The memorandum from the staff of the House Committee on Financial Services invokes yet another provision.[120] That is 18 U.S.C. § 1030, entitled "Fraud and related activity in connection with computers."[121] In searching for a provision that might cover "fraudulent comments" submitted by bots, this sounds promising. But at its core, the law is aimed at a very different kind of activity: accessing a computer without authorization and obtaining information or data—in a word, hacking. Courts have varied significantly in how broadly to read its provisions; some read it to prohibit use of a public website in a manner inconsistent with its terms of use, others limit it to situations of actual

---

116 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 18 U.S.C. § 1037 (2018).

117 *Id.* § 1037(a)(2).

118 *Id.* § 1037(d)(4).

119 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7702(2)(A) (2018).

120 Memorandum from Majority Staff of House Committee on Financial Services to Members of the Committee 2, n.10 (Feb. 3, 2020), https://financialservices.house.gov/uploadedfiles/hhrg-116-ba09-20200206-sd002.pdf [https://perma.cc/KM68-M4J9].

121 This provision was adopted in the Comprehensive Crime Control Act of 1984 and then substantially amended just two years later by the Computer Fraud and Abuse Act (CFAA); it has been amended eight times since, most recently in 2008.

harmful hacking.[122] The ultimate goal is protecting information housed on private or government computers.[123] So most of it is plainly inapplicable.[124]

The one provision that might apply is subsection (a)(4), which makes it a crime to access a computer without authorization or in exceedance of authorization with intent to defraud.[125] Online submissions of malattributed comments use a computer—two, actually: the sender's and the government's—and if the submission is an effort to "defraud" perhaps we have discovered a violation. I have argued above that such comments are not properly understood as an effort to defraud, strictly speaking. But courts have been quite loose in their understanding of "defraud" in this setting, explicitly holding that common-law fraud does not have to be shown.[126] But the reason that is so is that, in keeping with the nature of the provision as a whole, the core of the offense is not "fraud" but the unauthorized access of someone else's computer and the obtaining something of value. The legislative history confirms what the text indicates: Congress did *not* seek to criminalize any fraud that was conducted using a computer; it explicitly rejected proposals to pattern the new law on the mail and wire fraud statutes.[127]

> To be prosecuted under [section 1030(a)(4)], the use of the computer must be more directly linked to the intended fraud. That is, it must be

---

122 The cases are discussed in Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143 (2016). Kerr argues that the best understanding of this and similar statutes is by analogy to physical trespass. Under his approach, filing malattributed comments would not seem to violate the statute since the submitter has merely entered publicly available "space" at the invitation of the agency.

123 *See* HiQ Labs v. LinkedIn, 938 F.3d 985, 1001 (9th Cir. 2019) (citing S. REP. NO. 104-357, at 7 (1996)).

124 A useful summary is OFFICE OF LEGAL EDUCATION, EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS, PROSECUTING COMPUTER CRIMES (2015).

125 This section makes it a crime when someone "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." 18 U.S.C. § 1030(a)(4) (2018).

126 *See* Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc., 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008) ("The term 'defraud' for purposes of § 1030(a)(4) simply means wrongdoing and does not require proof of common law fraud.").

127 S. REP. NO. 99-432, at 9 (1986).

> used by an offender without authorization or in excess of his authorization to obtain property of another, which property furthers the intended fraud.[128]

Thus, the reference to an intent to defraud and obtaining a thing of value separate this subsection from earlier provisions that criminalized, as misdemeanor rather than felony, simply accessing and obtaining information from someone's computer. The "intent to defraud" language is inartful, but the legislative history makes clear that the fundamental concern was hacking into a computer and obtaining/stealing information, and that the offense was more serious when that information was used to obtain a thing of value.[129]

Accordingly, even if malattributed commenters have an intent to defraud, they have not violated the CFAA. The provision requires that the defendant "access a computer" "without authorization" or "exceed authorized access" and then obtain a thing of value. That is not what is happening. First, virtually no information is obtained. Second, while going on to regulations.gov or uploading comments to the FCC's Electronic Comment Filing System does involve "accessing a computer,[130] that is not done "without authorization;" every member of

---

128 *Id.*

129 In the words of the Senate Report:

> The Committee remains convinced that there must be a clear distinction between computer theft, punishable as a felony [under subsection (a)(4)], and computer trespass, punishable [under subsection (a)(2)] in the first instance as a misdemeanor. The element in the new paragraph (a)(4), requiring a showing of an intent to defraud, is meant to preserve that distinction, as is the requirement that the property wrongfully obtained via computer furthers the intended fraud.

Id. at 10; *see also* 132 CONG. REC. 7128, 7189 (1986) ("The acts of fraud we are addressing in proposed section 1030(a)(4) are essentially thefts in which someone uses a Federal interest computer to wrongfully obtain something of value from another . . . Proposed section 1030(a)(4) is intended to reflect the distinction between theft of information, a felony, and mere unauthorized access, a misdemeanor.") (statement of Sen. Laxalt).

130 One other question is whether, even if it is accessing a computer, it is accessing a "protected computer," as the statute requires. That is a term of art and the definition does not seem to reach the public portions of a government website. 18 U.S.C. § 1030(e)(2)(A) (2018). On the other hand, any computer that is used in or affecting interested commerce is also a "protected computer." *Id.* § 1030(e)(2)(B). Some courts have held that any time a person uses the Internet that requirement is met. *See, e.g.*, United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007). None of these cases involved government websites. If any computer, governmental or private,

the public is authorized to use the site to submit comments. Now, one could argue that if commenters are not authorized to post pseudonymous comments (explicitly? implicitly?) the poster exceeds authorized access by accessing the site for this impermissible (unauthorized) purpose. In some settings, courts have accepted such an argument.[131] But that argument, which is already at the outer bounds of judicial readings of the statute,[132] proves too much in this setting. Any violation of the agency's guidelines for commenting—page limits, deadlines, format, relevance—now becomes a federal crime.

The CFAA is likely inapplicable for one last reason. A violation requires not just an intent to defraud but that the person "by means of such conduct furthers the intended fraud and obtains anything of value." If we assume that there is fraud here (a big "if"), there is still no violation unless the commenter has actually "obtain[ed] anything of value." That is not a defined term, but against the background of traditional fraud, *McNalley*, the overall legislative history of the Act, and the text itself, the "thing of value" would seem to be not an indirect ultimate goal, but something that is actually found on the computer that has been accessed without authorization, such as credit card numbers, a competitor's trade secrets, or customer's email addresses. It is hard to fit a desired regulatory

connected to the Internet is a "protected computer" then this conduct does involve protected computers.

131 *See, e.g.*, EarthCam, Inc. v. OxBlue Corp., 703 F. App'x. 803, 808 (11th Cir. 2017) (suggesting that "a person exceeds authorized access if he or she uses the access in a way that contravenes any policy or term of use governing the computer in question"); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) ("Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."). *But see* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) ("[A] violation of the terms of use of a website—without more—cannot establish liability under the CFAA.").

132 Orin Kerr proposes a useful and sensible test for when accessing a website is without authorization. Drawing on the web's norm of openness, he suggests that the authorization line should be deemed crossed only when access is gained by bypassing an authentication requirement. An authentication requirement, such as a password gate, is needed to create the necessary barrier that divides open spaces from closed spaces on the Web. This line achieves an appropriate balance for computer trespass law. It protects privacy when meaningful steps are taken to seal off access from the public while also creating public rights to use the Internet free from fear of prosecution. Kerr, *supra* note 122, at 1161. Under this standard, submission of malattributed comments, however problematic, and even if in violation of explicit agency instructions with regard to the filing of comments, just is not a violation of the statute.

outcome into that box, *even if it could be shown that such an outcome was obtained*, which it almost certainly could not.

d. Conspiracy to Defraud the United States—Impairing Government Functions

For a century and a half, federal law has made it a crime to conspire to defraud the United States.[133] The current version, 18 U.S.C. § 371, dates to 1948.[134] It makes it a crime to "conspire either to commit any offense against the United States, *or to defraud the United States,* or any agency thereof in any manner or for any purpose."[135] A conspiracy to defraud the United States, as opposed to a conspiracy to commit a specific offense against the United States, is generally referred to as a "*Klein* conspiracy."[136] The meaning of "defraud" under § 371 is broader than its definition at common law or in the federal mail and wire fraud statutes.[137] Section 371 is not limited to schemes that deprive the government of money or property,[138] it reaches "any conspiracy for the purpose of

---

133 *See* Act of March 2, 1867, ch. 169, § 30, 14 Stat. 484 (prohibiting conspiracy to "defraud the United States in any manner whatsoever").

134 Pub. L. No. 80-772, ch. 645, 62 Stat. 683, 701 (1948) (codifying Title 18 into positive law). On the background of the current provision, see H.R. REP. NO. 304, at A28–29 (1947).

135 18 U.S.C. § 371 (2018) (emphasis added). The provision reads in full:

> If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined not more than $10,000 or imprisoned not more than five years, or both. If, however, the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor.

Id.

136 *See* United States v. Klein, 247 F.2d 908 (2d Cir. 1957); *see generally* Gretchen C.F. Shappert & Christopher J. Costantini, *Klein Conspiracy: Conspiracy to Defraud the United States*, 61 U.S. ATT'YS' BULL. 1 (July 2013).

137 *See* Dennis v. United States, 384 U.S. 855, 861 (1966) ("It has long been established that this statutory language is not confined to fraud as that term has been defined in the common law."); United States v. Ballistrea, 101 F.3d 827, 831 (2d Cir. 1996) (noting that "it is well established that the term 'defraud' as used in section 371 is 'interpreted much more broadly than when it is used in the mail and wire fraud statutes.'") (quoting United States v. Rosengarten, 857 F.2d 76, 78 (2d Cir. 1988)).

138 *E.g.*, Hammerschmidt v. United States, 265 U.S. 182, 188 (1924) ("To conspire to defraud the United States means primarily to cheat the government out of property or money, but it also

impairing, obstructing, or defeating the lawful function of any department of Government."[139] That language—"impair, obstruct or defeat a lawful governmental function"—dates to a 1910 Supreme Court decision[140] and is not actually in the statute, but is widely invoked as if it is.[141] And it is extraordinarily broad. That breadth creates room for creative possible uses of "the prosecutor's darling,"[142] but is also unsettling and counsels some caution.[143] In any event, because the caselaw is so expansive and untied to the statutory term ("defraud"), § 371 seems the most promising of the federal fraud provisions to apply in this setting.

Submission of millions of (unique) comments does impede a lawful government function. The deluge makes it harder for the agency to get a rule out the door, which delays the regulatory benefit or relief from restriction the rule provides. But that alone does not violate § 371 because there is no element of trick or deceit.[144] To find a violation, it is necessary to identify how exactly the use of a phony name on one, or a million,

---

means to interfere with or obstruct one of its lawful government functions . . . ."); United States v. Puerto, 730 F.2d 627, 630 (11th Cir. 1984).

139 Haas v. Henkel, 216 U.S. 462, 479–80 (1910) (upholding convictions under this provision where the defendants had submitted false information to the Department of Agriculture, thereby skewing its published statistics).

140 *Id.* at 479.

141 *See, e.g.*, Tanner v. United States, 483 U.S. 107, 128 (1987) (noting that Section 371 reaches "any conspiracy for the purpose of impairing, obstructing or defeating the lawful function of any department of Government"); United States v. Nersesian, 824 F.2d 1294, 1313 (2d Cir. 1987) (citing Hammerschmidt v. United States, 265 U.S. 182, 188 (1924)) ("[T]he crime of conspiracy to defraud the United States includes acts that interfere with or obstruct one of its lawful governmental functions by deceit, craft, or trickery, or by means that are dishonest.").

142 *See, e.g.*, William C. Tucker, *Deceitful Tongues: Is Climate Change Denial a Crime?*, 39 ECOL. L.Q. 831, 878–91 (2012) (arguing that coordinated efforts to mislead the public and government regulators regarding the seriousness of climate change violate § 371). It was Learned Hand who referred to conspiracy as "that darling of the modern prosecutor's nursery." Harrison v. United States, 7 F.2d 259, 263 (2d Cir. 1925).

143 For criticism, see Jeremy H. Temkin, *Time to Revisit the 'Klein' Conspiracy Doctrine*, N.Y.L.J. (Jan. 25, 2013), https://www.maglaw.com/publications/articles/2013-01-25-time-to-revisit-the-klein-conspiracy-doctrine/_res/id=Attachments/index=0/Time%20to%20Revisit%20the%20%E2%80%98Klein%E2%80%99%20Conspiracy%20Doctrine.pdf [https://perma.cc/XAX5-DYFD].

144 *See, e.g.*, United States v. Caldwell, 989 F.2d 1056 (9th Cir. 1993) (holding that § 371 does not impose an obligation on individuals to make the government's job easier or to avoid obstructing government activity; the statute is triggered only when obstruction is accomplished through dishonesty or deceit).

comments obstructs the agency's functioning. The argument seems conceivable. Just as the Special Counsel's indictment of Russian conspirators alleged a violation of § 371 through the use of phony social media posts in order to derail and alter the outcome of the 2016 election,[145] so phony rulemaking comments can be seen as an effort to derail and alter the outcome of the rulemaking process. By making the agency think a raft of non-existent individuals support a particular outcome, the submitter is attempting to influence the final decision. For reasons set out above, it is unlikely to succeed in doing so, but that is irrelevant to the existence of a conspiracy to impair, obstruct, or defeat lawful functions. And if the agency is influenced by false information in a submission, its functions have been impeded or impaired in the sense that it failed to reach the "right" result.

Nonetheless, tying the trick or deceit to the obstruction is not straightforward. In the case of Russian election meddling, it was essential to the effect of the disinformation that people reading the posts *thought* they came from ordinary Americans rather than Russian bots or dissemblers. The whole impact depended on creating the impression that lots of Americans possessed certain information, doubts, and beliefs. If each post were clearly identified as coming from the Internet Research Agency, the effect would have been lost. That is just not the case with malattributed comments; the impact does not hinge on the commenter's identity. It should not even hinge on the belief that there is an actual commenter behind the comment.

Moreover, using a false identity on a comment is quite different from lying on one's tax return, or submitting false information about campaign contributions to the Federal Election Commission, or giving a police officer a phony name. In general, *Klein* conspiracies are charged in

---

145 Indictment ¶¶ 2, 28, United States v. Internet Research Agency, No. 1:18-cr-00032-DLF (D.D.C. Feb 16, 2018) (alleging conspiracy "to defraud the United States by impairing, obstructing, and defeating the lawful functions of the government through fraud and deceit for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016"). The sufficiency of the indictment was upheld in United States v. Concord Management & Consulting LLC, 347 F. Supp. 3d 38 (D.D.C. 2018). Notably, the court had reservations about the claim that affirmative misrepresentations (as opposed to a refusal to comply with statutorily imposed reporting obligations) would obstruct legitimate government functions. "The difficulty for the government . . . is not *identifying* deceit—of which there is plenty—but *connecting* that deceit to [a particular] lawful government function . . . which the defendants allegedly conspired to impair." *Id.* at 51.

tax cases;[146] another common setting involves the failure to disclose information to the government when there is a legal obligation to disclose.[147] Those standard § 371 "impairments" all directly obstruct agency enforcement activities. Additionally, the impossibility of showing substantial harm to the federal government or an agency will disincline any prosecutor to pursue such a case.

Finally, the crime here is not making the false statements, it is conspiracy. So any actual prosecution would have to show an agreement between multiple people. That will often but not always be possible.

e. Obstructing Agency Proceedings

The cluster of criminal provisions regarding obstruction of justice[148] includes a prohibition on obstructing proceedings before agencies and departments.[149] There is a sense, as the prior section indicates, in which submission of an malattributed comment "obstructs" an agency "proceeding." However, the *text* of this provision, as opposed to its title, make it a poor fit. As one would expect from its placement in a set of provisions regarding obstruction of justice, the section is aimed at agency

---

146 *See, e.g.*, United States v. McKee, 506 F.3d 225 (3d Cir. 2007).

147 *See* United States v. Murphy, 809 F.2d 1427, 1431–32 (9th Cir. 1987) ("Where the regulations implementing the Act [administered by the agency] do not impose a duty to disclose information, failure to disclose is not conspiracy to defraud the government.").

148 18 U.S.C. §§ 1501 *et seq.* (2018).

149 *Id.* § 1505. The provision provides, in full:

> Whoever, with intent to avoid, evade, prevent, or obstruct compliance, in whole or in part, with any civil investigative demand duly and properly made under the Antitrust Civil Process Act, willfully withholds, misrepresents, removes from any place, conceals, covers up, destroys, mutilates, alters, or by other means falsifies any documentary material, answers to written interrogatories, or oral testimony, which is the subject of such demand; or attempts to do so or solicits another to do so; or
>
> Whoever corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States, or the due and proper exercise of the power of inquiry under which any inquiry or investigation is being had by either House, or any committee of either House or any joint committee of the Congress—
>
> Shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both.

investigations and adjudications, the counterpart to criminal investigations and trials that are the setting for most obstruction of justice violations. No case has held that a notice-and-comment rulemaking is a "proceeding" within the meaning of this section. Many cases assert that "proceeding" is to be read broadly.[150] But what they mean is that the term is not limited to an actual adjudication but extends to the whole investigatory process that precedes it.[151]

Even if a rulemaking qualifies as an agency "proceeding," submitting a phony or malattributed comment does not reach the level of obstruction necessary. A violation of the first paragraph consists in withholding or misrepresenting information in response to "any civil investigative demand duly and properly made under the Antitrust Civil Process Act." Notice-and-comment rulemaking fails on both counts: there is no demand and the Antitrust Civil Process Act is irrelevant. A violation of the second paragraph requires intimidating conduct—such as and including threats and force—that goes far beyond simple submission of a comment with the wrong person's name on it.[152]

B. *Making False Statements*

Moving away from fraud-based crimes, the obvious basis for a possible prosecution is the ever-helpful prohibition on making "false, fictitious, or fraudulent" statements to a federal agency found at 18 U.S.C. § 1001.[153] Most elements of the crime are clearly satisfied here. Though

---

150 *See, e.g.*, United States v. Leo, 941 F.2d 181, 198–99 (3d Cir. 1991); United States v. Mitchell, 877 F.2d 294, 300 (4th Cir. 1989) (noting that "decisions have uniformly held that th[e] term ['administrative proceeding'] should be construed broadly to effectuate the statute's purpose").

151 *See, e.g.*, United States v. Vixie, 532 F.2d 1277 (9th Cir. 1977); Rice v. United States, 356 F.2d 709, 712 (8th Cir. 1966) ("[I]t would be absurd to hold that Congress meant to proscribe interference with the administrative process only after a Labor Board proceeding had reached a certain formal stage and let go unpunished individuals who obstruct earlier preliminary proceedings by frightening witnesses into withdrawing charges out of fear for their lives. Congress clearly intended to punish any obstruction of the administrative process by impeding a witness in any proceeding before a governmental agency—at any stage of the proceedings, be it adjudicative or investigative.").

152 18 U.S.C. § 1505 (2018).

153 As amended in 1996, this section provides:

not "fraudulent,"[154] a malattributed comment does make a "false" and "fictitious" "statement or representation" in asserting that it is submitted by someone other than the actual submitter. In addition, the falsehood is knowing or willful. It is true that whoever is programming the computer or authorizing the submissions does not know of each specific misidentification, but that person does know that the misidentifications are being made.

Next, a notice-and-comment rulemaking is "a matter within the jurisdiction" of the agency conducting the rulemaking. While that caselaw has historically produced some counterintuitive results,[155] even where courts have read the term "jurisdiction" narrowly, they have frequently pointed to writing regulations as the sort of activity that *is* within an agency's jurisdiction.[156] And the Supreme Court has more than once admonished that the term should not be read technically or narrowly.[157] A notice-and-comment rulemaking is a setting in which the

---

> Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully—
>
> (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact;
>
> (2) makes any materially false, fictitious, or fraudulent statement or representation; or
>
> (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry;
>
> shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both. If the matter relates to an offense under chapter 109A, 109B, 110, or 117, or section 1591, then the term of imprisonment imposed under this section shall be not more than 8 years.

18 U.S.C. § 1001(a) (2018).

154 *See supra* Section IV.A.

155 For example, the Eighth Circuit once held that falsely telling the FBI that one's missing wife is involved in a plot to kill the President in order to induce the Bureau to go looking for her does not involve a matter within the FBI's jurisdiction. United States v. Rogers, 706 F.2d 854 (8th Cir. 1983). The Supreme Court unanimously reversed, holding that investigations by federal agents are "matter[s] within the jurisdiction of a[] department or agency of the United States." United States v. Rodgers, 466 U.S. 475, 484 (1984).

156 *See, e.g.*, Friedman v. United States, 374 F.2d 363, 368 (8th Cir. 1967) (explaining that "jurisdiction" involves such things as the "power to adjudicate rights, establish binding regulations, compel the action or finally dispose of the problem giving rise to the inquiry").

157 *Rogers*, 466 U.S. at 480; Bryson v. United States, 396 U.S. 64, 70–71 (1969).

rulemaking agency has the "power to exercise authority,"[158] both in the sense of conducting the rulemaking and in the sense of issuing a regulation, and accordingly is a matter within the agency's jurisdiction.

One might argue that these false statements—or, more precisely, the falsity of these statements—have no impact on the agency. FCC Chair Ajit Pai, for example, certainly would say—he did say[159]—that the FCC was not misled or even distracted by the millions of malattributed comments. However, if this ineffectualness matters, it is relevant to materiality, discussed below. The mere fact that the false statement was ineffective in the individual instance does not mean the statute was not violated. Section 1001 does not require that the government rely on or be influenced by the statement,[160] not realize that it was false,[161] or suffer pecuniary loss due to the statement.[162]

That leaves the central question—central to the § 1001 issue and central to the larger inquiry: is the falsehood "material"?[163] Under the standard formulation, a statement is material under § 1001 if it "'has a natural tendency to influence, or [is] capable of influencing, the decision of the decision-making body to which it was addressed."[164] A statement can be material even if the agency was not actually misled or deceived and

---

158 United States v. Davis, 8 F.3d 923, 929 (2d Cir. 1993).

159 Letter from Ajit Pai, FCC Chairman, to Michael E. Capuano, U.S. Representative, *supra* note 17 ("Despite any suggestion that the public comment process was somehow 'flawed' or 'tampered with' by the alleged submission of comments under false names, any such activity did not affect the Commission's actual decision-making . . .").

160 *See, e.g.*, United States v. Clay, 832 F.3d 1259, 1309 (11th Cir. 2016); United States v. Trent, 949 F.2d 998 (8th Cir. 1991); United States v. Boone, 951 F.2d 1526 (9th Cir. 1991); Nilson Van & Storage Co. v. Marsh, 755 F.2d 362 (4th Cir. 1985).

161 *Clay*, 832 F.3d at 1309 (quoting United States v. Neder, 197 F.3d 1122, 1128 (11th Cir. 1999)).

162 *See, e.g.*, United States v. Godel, 361 F.2d 21 (4th Cir. 1966); United States v. Hawkins, 295 F.2d 837 (6th Cir. 1961).

163 As originally enacted, the statute explicitly required materiality only with regard to falsifying, concealing, or covering up a fact. The circuits split as to whether to read the requirement into the prohibitions on false statements or writings. Congress resolved the split in the False Statements Accountability Act of 1996, Pub. L. No. 104-292, § 2 (1996), separately enumerating the three types of violation and making materiality an explicit requirement for each.

164 Neder v. United States, 527 U.S. 1, 16 (1999); Kungys v. United States, 485 U.S. 759, 770 (1988) (summarizing lower court rulings); United States v. Norris, 749 F.2d 1116 (4th Cir. 1984). Construing the same term in a different but similar provision, the *Kungys* Court adopted this formulation: "whether the misrepresentation or concealment was predictably capable of affecting, i.e., had a natural tendency to affect, the official decision." *Kungys*, 485 U.S. at 771.

in fact did not rely on the falsehood; it suffices if the falsehood would have "a natural tendency" to influence, or be capable of affecting or influencing, a governmental decision.[165]

Does the effect or influence of a comment hinge on who submitted it? Would or should or, most importantly, does an agency treat a comment from Joe Smith differently than one from Susan Jones? If not, then the false name is not "material." I will not repeat the discussion from Section IV.A, but the point is that what matters is the content of the comment, not the identity of its author. Using random names from the phone book to misidentify the source of a comment is therefore not a material misstatement.

A subcategory of malattributed comments would violate § 1001, however. Suppose a comment falsely claims to be from someone with extensive relevant expertise and experience—a Ph.D. research chemist, a twenty-year line employee in the relevant industry, a user of a product the agency proposes to ban, the owner of property in the neighborhood of a regulated facility. Because the person's supposed unique, relevant experience would give the comment more weight, that misstatement would be material. And if simply by using a particular person's name that information about background could be communicated, then just the false name would be material. However, the sort of malattributed comments that are controversial are not this kind of thing at all. They are duplicative and generic, make no representations as to background or expertise, and do not use recognizable names of experts.

C. *Identity Theft*

In the wake of the net neutrality rulemaking Senator Rob Portman complained: "Victims of identity theft are being misrepresented on federal government websites, and agencies are doing little to protect them."[166] The term "identity theft" gets tossed around quite a bit in these

---

165 U.S. v. Markham, 537 F.2d 187 (5th Cir. 1976).

166 Press Release, Portman, Carper: Bipartisan Report Highlights Abuse of Online Regulatory Comment Systems (Oct. 24, 2019), https://www.portman.senate.gov/newsroom/portman-carper-bipartisan-report-highlights-abuse-online-regulatory-comment-systems [https://perma.cc/Z5QL-UJWR].

discussions.[167] Too much. The term packs a punch but is not legally accurate. The core instances of identity theft involve taking something much less abstract than just a person's "identity." The contents of their bank account, for example. Calling malattributed comments identity theft is a nice rhetorical move, but it is both misleading and legally unfounded.

The federal government and all states have criminal prohibitions on certain uses of another's personally identifying information, and these are referred to, at least colloquially and sometimes statutorily, as "identity theft." There is no single legal definition. The classic form of "identity theft" is the use of another's credit card, bank account, or identification documents in order to get money or use the victim's credit to purchase goods. Thus, there is a tangible, concrete benefit to the thief and/or harm to the victim. As the leading practitioner's guide puts it:

> Succinctly stated, identity theft is the stealing of personal identification information which belongs to another (the victim-owner of the information), with the intent and for the purpose of fraudulently using the information to gain money, goods, services, or other economic or private benefit realized by the identity thief and any coconspirators.
>
> There are two components of identity theft: (1) the stealing of personal identification information belonging to another; and (2) the

167 *See, e.g.*, U.S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, *supra* note 122, at 3 (objecting that the FCC lacks adequate remedies for "identity theft victims" as allowing them to post a responsive or clarifying comment "potentially causes additional harm to victims of identity theft"); Nicholas Confessore, *New York Attorney General Expands Inquiry Into Net Neutrality Comments*, N.Y. TIMES (Oct. 17, 2018), www.nytimes.com/2018/10/16/technology/net-neutrality-inquiry-comments.html [https://perma.cc/5TMG-FLS4] ("[M]any comments on net neutrality were falsely submitted under the names of real people, in what amounted to mass acts of virtual identity theft."); U.S. Senate Permanent Subcommittee on Investigations, Press Release (Oct. 24, 2019), https://www.hsgac.senate.gov/subcommittees/investigations/media/carper-portman-bipartisan-report-highlights-abuse-of-online-regulatory-comment-systems [https://perma.cc/XUB8-Y2C5] ("Examples of the misuse of the online regulatory commenting system include rampant use of stolen identities to post comments on proposed regulations with no recourse for identity theft victims . . . ."); Linder, *supra* note 5 (quoting Pennsylvania AG Josh Shapiro referring to "massive identity theft"); Max Weiss, *Deepfake Bot Submissions to Federal Public Comment Websites Cannot Be Distinguished from Human Submissions*, TECHNOLOGY SCIENCE (Dec. 18, 2019), https://techscience.org/a/2019121801 [https://perma.cc/A3BH-ZEUC] ("Comments [in the net neutrality rulemaking] came from email addresses, street addresses, and postal codes stolen from unwitting victims, constituting countless instances of identity theft.").

> fraudulent misuse of such information to economically enrich or benefit the identity thief.[168]

For example, Wisconsin criminalizes the unauthorized use of someone's personal identifying information or documents

> (a) To obtain credit, money, goods, services, employment, or any other thing of value or benefit.
>
> (b) To avoid civil or criminal process or penalty.
>
> (c) To harm the reputation, property, person, or estate of the individual. [169]

It would be hard to prosecute malattributing commenters under this statute. The comment does indeed "use" someone's personal identifying information—their name. But what makes that a crime is the purpose for which it is done. "Influencing a federal rulemaking" does not come within the three prohibited purposes. Yes, favorable federal policy is in a sense "a thing of value." But if ever *ejusdem generis* would seem to be appropriate, it is here. The enumerated things of value are all tangible items belonging to the person whose identity is stolen. Thus, identity theft is a means, not an end; the harm that is of concern is not the intangible intrusion or some change in the outside world; it is the loss of or damage to something belonging to the victim.

Federal law is not more helpful. The staff of the House Financial Services Committee has suggested—albeit with a protective "could arguably"—that filing malattributed comments violates the federal identity theft statute codified at 10 U.S.C. § 1028.[170] This is quite a stretch.

---

168 Daniel J. Penofsky, *Litigating Identity Theft Cases*, 112 AM. JUR. TRIALS 1, § 7 (2009; updated 2020) (footnotes omitted). *See also* Keith B. Anderson, Erik Durbin & Michael A. Salinger, *Identity Theft*, 22 J. ECO. PERSPECTIVES 171, 174–75 (2008) (categorizing identity theft into three buckets: misuse of a credit card, use of someone else's identity to open new accounts in their name or take out loans, and use of someone else's name to access existing, but not open new, accounts).

169 Wis. Stat. § 943.201. California is broader: "Every person who willfully obtains personal identifying information . . . of another person, and uses 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, is guilty of a public offense." Cal. Penal Code § 530.5(a).

170 *See* Memorandum, *supra* note 120, at 2 & n.10.

The original federal statute, enacted in 1982,[171] was not about the theft of identity in the contemporary sense at all; it was about theft of *identification*. It made it a crime to produce, possess, or transfer a fake or someone else's ID. That has nothing to do with malattributed comments. As amended, the statute reaches further, but is still all about the use of documents or other "authentication features" such as holograms, symbols, a sequence of numbers of letters, or other such item issued by some sort of issuing authority. It is not about just pretending to be someone you are not.

The only plausible argument under § 1028 rests on a provision that makes it a crime to

> knowingly transfer[] . . . or use[], 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.[172]

The most obvious sorts of "means of identification" are ID cards of one sort or another. Filing a comment under someone else's name does not involve the use of an ID card. But the statutory definition of "means of identification" is broader, extending to "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including "any . . . name."[173] Just using someone else's *name*, without more, could theoretically constitute the "use" of a "means of identification" as long as that name can be used to identify a specific individual.

However, just using someone else's name is not the crime. The use must be in connection with some *other* activity that is itself a crime—indeed, a felony. So this provision just returns us where we began: is it a felony to file malattributed comments? If so, it is a felony that violates not one statute but two; but this section does not make it so.

---

171 False Identification Crime Control Act of 1982, P.L. No. 97-398, 96 Stat. 2009 (1982), codified at 18 U.S.C. § 1028.

172 18 U.S.C. § 1028(a)(7) (2018).

173 *Id.* §§ 1028(d)(7), (d)(7)(A).

In 2004 Congress passed the "Identity Theft Penalty Enhancement Act,"[174] prohibiting "aggravated identity theft."[175] Aggravated identity theft occurs when someone "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person" in connection with a set of enumerated felonies, all of which involve obtaining money or other benefits through fraud.[176] Like the provision in § 1028 just discussed, this offense is parasitic; it requires commission of a separate, enumerated felony. In effect, then, it enhances the punishment for another offense; it is not a stand-alone crime. For example, the Special Counsel's indictment of the Internet Research Agency et al. alleged conspiracy to defraud the United States (count I), conspiracy to commit mail and wire fraud (count II), and aggravated identity theft (counts III–VIII) in that the defendants used "a means of identification of another person"—social security numbers, dates of birth, home addresses—"during and in relation to" the felonies of wire and bank fraud.

In our situation, the most obvious predicate offense would be making a false statement, and the statute's enumeration of covered offenses does indeed include 18 U.S.C. § 1001. Aggravated identity theft occurs if "during and in relation to" that felony a person "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person."[177] Again, the most obvious examples, in which the thief passes off a stolen or fake card, are inapplicable here. But this section too defines the term "means of identification" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual."[178] Simply giving a name can involve the use of a "means of identification" so long as the name could be combined with other information to identify a specific individual. So, for example, forging a payee's signature on the back of a check constitutes a "means of identification."[179] Most names, with no other identifying information, would not be a "means of identification," because most names are insufficiently unique. So, in our setting, a

174 Pub. L. No. 108-275, 118 Stat. 831 (2004), codified at 18 U.S.C. § 1028A.

175 18 U.S.C. § 1028A (2018) (heading).

176 18 U.S.C. § 1028A(a)(1) (2018).

177 *Id.*

178 18 U.S.C. § 1028(d)(7) (2018).

179 United States v. Morel, 885 F.3d 17, 22–23 (1st Cir. 2018) (citing cases); United States v. Wilson, 788 F.3d 1298, 1310–11 (11th Cir. 2015).

comment that says it was submitted by "John Smith" does not involve use of a "means of identification," because the name alone is not enough to pinpoint a specific individual.[180] But the name as well as an address (street or email), for example, could suffice. So a number of malattributed comments arguably involve the "use[], without lawful authority, [of] a means of identification of another person." Still, that is not a violation of the statute. That use must be "during and in relation to" one of the enumerated felonies.[181] If no other crime has occurred, as I have argued, then there is also no aggravated identity theft.

D. *Criminal Impersonation*

Most or all states have laws criminalizing false impersonation. All require impersonation of a real individual for the purpose of gaining a benefit or causing an injury.[182] Former New York Attorney General Eric Schneiderman suggested that malattributed comments may violate the relevant provisions of the New York Penal Law.[183]

In New York, impersonation in the second degree consists of "[i]mpersonat[ing] another and do[ing] an act in such assumed character with intent to obtain a benefit or to injure or defraud another,"[184] and specifically includes a prohibition on "[i]mpersonat[ing] another by communication by internet website or electronic means with intent to obtain a benefit or injure or defraud another."[185] "Impersonation" occurs when one person assumes the identity of another particular individual; it

---

180 "A name alone, for example, would likely not be sufficiently unique to identify a specific individual because many persons have the same name. Likewise, a date of birth by itself would not be sufficient because multitudes of persons are born on the same day." United States v. Mitchell, 518 F.3d 230, 234 (4th Cir. 2008).

181 18 U.S.C. § 1028A(a)(1) (2018).

182 *See generally* Marie K. Pesando, 32 AM. JUR. 2D § 1, *False Personation*.

183 Eric Schneiderman, *An Open Letter to the FCC*, MEDIUM (Nov. 21, 2017) https://medium.com/@NewYorkStateAG/an-open-letter-to-the-fcc-b867a763850a [https://perma.cc/N5DY-URCQ] ("My office analyzed the fake comments and found that tens of thousands of New Yorkers may have had their identities misused . . . . Impersonation and other misuse of a person's identity violates New York law . . . .").

184 N.Y. PENAL LAW § 190.25(1) (McKinney 2020).

185 *Id.* § 190.25(4). First degree impersonation is limited to certain egregious acts when pretending to be a law enforcement officer or prescribing physician and is plainly inapplicable here. *See id.* § 190.26.

does not violate the statute to "simply use[] some fictitious or assumed name."[186] Thus comments with fictitious names would not violate the statute. Nor would the use of a name that happens to exist in the real world but cannot be linked to any particular individual who bears that name. However, a comment that used a real person's name *along with* an email or mailing address would count as "impersonation." And submission of an electronic comment is a "communication by website or electronic means."

But impersonation alone is not a crime; the impersonation must be with the intention to injure or defraud another. As discussed above, malattributed comments are not fraudulent in any recognized sense. As for injury, those whose identities were used *feel* injured. But it is unlikely, and impossible to prove, that the submitter acted with the *intent* of injuring the person whose name was used. Conceivably the injury is inflicted knowingly, but knowingly is not the same as intentionally.

Furthermore, it is not clear that the "injury" suffices. Injury is not limited to pecuniary harm. Reputational harm surely counts, for example. But the injury must be real and consequential. In the leading recent case, the New York Court of Appeals concluded that "the statutory terms 'injure' and 'benefit' cannot be construed to apply to *any* injury or benefit, no matter how slight;" rather, "intent . . . to injure" requires an intent to cause "real harm" or "substantial harm."[187]

Conceivably a net neutrality enthusiast, particularly one engaged in public debate, might suffer a reputational harm by being associated with an anti-net neutrality filing. But any such harm is awfully minor and easily combatted. The very visibility that arguably creates the problem (a) dilutes it (because no one paying attention will be fooled by the comment) and (b) is the means of solving it.[188] As noted in Part IV,[189] the most compelling example, unlikely and so far only hypothetical, would be a malattributed comment containing offensive or abhorrent content that goes viral, which really could result in irremediable and serious reputational harm.

---

186 People v. Chive, 734 N.Y.S.2d 830, 833 (N.Y. Crim. Ct. 2001); *see also* People v. Sadiq, 654 N.Y.S.2d 35 (N.Y. App. Div. 1997).

187 People v. Golb, 15 N.E.3d 805, 812–13 (2014) (emphasis in original).

188 As, for example, Karl Bode has shown. *See* Bode, *supra* note 57.

189 *See supra* Section IV.D.

Conceivably the submitter of a malattributed comment is seeking "to obtain a benefit" in the form of a preferred policy outcome.[190] Again, this is a far cry from the standard forms of benefit, which are pecuniary or at least tangible. The two most common are getting money or avoiding prosecution.[191] The benefit here is far more abstract and attenuated.[192]

Perhaps the most interesting theory under which these submissions might amount to criminal impersonation would be that the "injury" is interference with the government's ability to do its job. The New York courts have frequently set out some variation of the following black-letter proposition: "a person may be found guilty of criminal impersonation in the second degree if he or she impersonates another with the intent to cause a tangible, pecuniary injury to another*, or the intent to interfere with governmental operations*."[193] There is a sense in which the comment is such an effort, as I discussed above in the context of 18 U.S.C. § 371.[194] Still, this theory faces an uphill battle. First of all, the key language is not in the statute itself, it only shows up in opinions explaining the kind of harm that the statute protects against. Second, this setting is enormously different from that in the New York cases that invoke the interference with governmental operations theory; those cases all involve the police or the courts. Examples include driving with someone else's license, giving an arresting officer someone else's name,[195] pretending to be the victim of a crime and telling the police you do not wish to press charges,[196] or

190 The Penal Law defines "benefit," not very helpfully, as "any gain or advantage to the beneficiary and includes any gain or advantage to a third person pursuant to the desire or consent of the beneficiary." N.Y. PENAL LAW § 10.00(17) (McKinney 2020).

191 People v. Lynch, 34 N.E.3d 341, 344 (N.Y. 2015) ("With the [forged] non-driver ID card in hand, defendant could give the appearance of a clean record, which would enable him to evade his criminal history and obtain a loan or employment under a false identity."); People v. Chive, 734 N.Y.S.2d 830, 835 (N.Y. Crim. Ct. 2001); People v. Sherman, 455 N.Y.S.2d 528, 529 (N.Y. City Ct. 1982) (defendant admitted that he lied about his identity to arresting officer and threw away papers reflecting true identity "in order to avoid problems or prosecution under his real name"); People v. Pergolizzi, 400 N.Y.S.2d 1005 (N.Y. Sup. Ct. 1977).

192 Felix Wu has pointed out to me the analogy between this understanding of the requisite injury and related principles requiring concrete and particularized injuries (or lost benefits) in standing doctrines.

193 *Golb*, 23 N.Y.3d at 466 (emphasis added).

194 *See supra* notes 133–45 and accompanying text.

195 People v. Turner, 651 N.Y.S.2d 655 (N.Y. App. Div. 1996).

196 People v. Hooks, 896 N.Y.S.2d 501 (N.Y. App. Div. 2010).

impersonating an FBI agent.[197] These are all a far cry from submitting a malattributed comment in a federal rulemaking. It seems unlikely the New York courts would expand the scope of this inferred application of the statute so far.

E. *The Administrative Procedure Act*

The final potential legal issue arises not under a criminal provision but under the Administrative Procedure Act (APA). This is a very different sort of challenge. The APA applies to the agency, not the commenters, so the question is whether the APA requires agencies to reject, or prohibit, or cleanse the docket of malattributed comments.

In the wake of the *Wall Street Journal*'s reporting on the net neutrality rulemaking, several observers asserted that the notice-and-comment process was so defective that the rule was invalid.[198] Given

---

197 People v. Sanchez, 643 N.E.2d 509 (N.Y. 1994).

198 *See, e.g., Free Press Joins in Appeals Court Brief Against FCC's Unlawful and Unpopular Repeal of Net Neutrality Safeguards*, FREE PRESS (Aug. 21, 2018), https://www.freepress.net/news/press-releases/free-press-joins-appeals-court-brief-against-fccs-unlawful-and-unpopular-repeal [https://perma.cc/JF5N-GSWE] (statement of Matt Wood, Policy Director, Free Press) ("The agency likewise ignored evidence from tens of thousands of consumer complaints, and looked the other way when fraudulent comments filled its online filing system."); *Net Neutrality in the United States*, WIKIPEDIA, https://en.wikipedia.org/wiki/Net_neutrality_in_the_United_States [https://perma.cc/BRQ8-CHR9] ("[T]wenty two state Attorneys General filed suit against the FCC, alleging among other things that the comment process had been corrupted, making the rule changes invalid."); Melissa Quinn, *Millions of Phony Public Comments Muddle FCC's Net Neutrality Vote*, WASH. EXAMINER (Dec. 12, 2017, 12:01 AM), https://www.washingtonexaminer.com/millions-of-phony-public-comments-muddle-fccs-net-neutrality-vote [https://perma.cc/ERX4-XR3U]; Schneiderman, *supra* note 183 (objecting that "the perpetrator or perpetrators attacked what is supposed to be an open public process by attempting to drown out and negate the views of the real people, businesses, and others who honestly commented on this important issue"); *see also* Bob Barr, *Massive Fraud in Net Neutrality Process is a Crime Deserving of Justice Department Attention*, MARIETTA DAILY J. (Dec. 25, 2017), https://www.mdjonline.com/opinion/bob-barr-massive-fraud-in-net-neutrality-process-is-a-crime-deserving-of-justice-department/article_87a01d86-e9c5-11e7-af34-3bc55501c7a0.html ("[B]efore too long, the voices of real people, expressing genuine opinions on regulations, will be drowned out and ignored all together by those in power.").

Vermont Yankee,[199] this objection can only rest on the APA, and many voicing it specifically invoked the APA.[200]

But what exactly is the APA violation here? By definition those *submitting* malattributed comments are not violating the APA; it does not apply to them. If there is an APA violation, it must be in how the agency handles the comments. Yet the APA says very little about that. The basic APA obligation is that agencies *consider* the comments;[201] courts have broadened this obligation to require that in issuing a final rule agencies *respond* to all significant comments.[202] Given this, it is at least arguable that not only are agencies not required to police for malattributed comments, they must consider them. Of course, an agency may—usually will—conclude that the comment says nothing of value and does not require a response, and its malattribution could be one factor supporting that conclusion (though not a conclusive one). But lots of comments add nothing and go unresponded to. That does not mean the agency is under an affirmative obligation to keep them out of or remove them from the docket. Indeed, most useless comments *could not* be removed from the docket. First, doing so would be inconsistent with the right to comment. Second, doing so would make it impossible for a reviewing court to

---

199 Vt. Yankee Nuclear Power Corp. v. Natural Res. Def. Council, Inc., 435 U.S. 519 (1978) (holding that courts lack a general supervisory power over agency procedures and cannot impose or invent requirements not established by statute or the Constitution).

200 Lapowsky, *supra* note 79 ("There are real questions about the integrity of the docket that can and will be used against [the FCC] in court.") (quoting Gigi Sohn); Klint Finley, *FCC's Broken Comment System Could Help Doom Net Neutrality*, WIRED (Sep. 2, 2017, 10:00 AM), https://www.wired.com/story/fccs-broken-comments-system-could-help-doom-net-neutrality [https://perma.cc/TW6M-QUQ4] (quoting Gigi Sohn as stating that the agency might have an obligation under the APA to remove fake comments from the docket and that "[a]t a bare minimum, they should investigate these comments and if they can't actually remove the comments, they can and should disregard them as part of their consideration of record"); State AGs' Letter, *supra* note 16 (letter from nineteen state Attorneys General urging the FCC to delay action because "the well of public comment has been poisoned by falsified submissions" and seeming to take the position that it would violate the APA to consider such submissions).

201 *See, e.g.*, Lilliputian Sys., Inc. v. Pipeline & Hazardous Materials Safety Admin., 741 F.3d 1309, 1312 (D.C. Cir. 2014) ("An agency's failure to respond to relevant and significant public comments generally demonstrates that the agency's decision was not based on a consideration of the relevant factors.").

202 *See, e.g.*, Delaware Dep't of Nat. Resources & Envtl. Control v. EPA, 785 F.3d 1, 15 (D.C. Cir. 2015); Cement Kiln Recycling Coal. v. EPA, 493 F.3d 207, 225 (D.C. Cir. 2007); Am. Mining Cong. v. EPA, 965 F.2d 759, 771 (9th Cir. 1992); St. James Hosp. v. Heckler, 760 F.2d 1460, 1470 (7th Cir. 1985).

review the full record and determine, among other things, whether the agency had in fact considered and responded to all significant comments.[203]

It *would* be an APA violation to rely on malattributed comments inappropriately. (This is not a proposition limited to malattributed comments; it would violate the APA to rely on any comment inappropriately. The challenge is explaining what counts as "inappropriate.") For example, if the agency tallied comments, basing its decision on the level of support for this or that aspect of the rule, then it would violate the APA to rely on malattributed comments. But we need not go that far; it would already violate the APA to base its decision simply on the number of pro and con comments, regardless of their authenticity.

If the idea of "polluting" or "corrupting" the docket was not a metaphor but a reality, then there might be an APA violation. The Act anticipates that the notice-and-comment process provides the agency with relevant "data, views, and arguments." If malattributed comments somehow kept such input from the agency or made it impossible for the agency to evaluate or understand the authentic comments, then to issue a rule based on the "corrupted" docket would be an APA violation. It would be akin to basing, say, an emissions limit on a computer model and finding that there was a bug in the program so it spat out the wrong results. But the analogy just does not hold. To some extent, the malattributed comments can be identified and ignored; they do not somehow rub off on the authentic ones. But more important, as noted before, whether a comment is signed, anonymous, or pseudonymous, it says what it says; it will be useful or irrelevant depending on its content, not on the validity of the signature line. Therefore, it is not a violation of the APA to read or to rely on a comment submitted under a false name. As a question of administrative law, this arises not so much under § 553, which in no way restricts what the agency can consider or who it can listen to. It is a question of what counts as "reasoned decision-making" that is not arbitrary and capricious and therefore subject to judicial

---

203 *See* Dooling, *supra* note 75, at 917–20. Of course, an agency can set reasonable requirements—for example of civility or not revealing confidential information–for comments and police those requirements. *Id.* at 905–15. But comments in violation of those requirements are not merely unhelpful, they do affirmative harm. The affirmative harm from malattributed comments is much less clear, as discussed in *supra* Part III.

reversal under § 706(2)(a). It would not be reasoned decision-making to count comments or to be swayed by the identity of the commentator. But if a comment is relevant, factually accurate, and communicates something of value, there is nothing arbitrary and capricious in an agency making use of what it has to offer, regardless of whether the sender put someone else's name on it.

During the net neutrality fury, opponents of the rule promised that they would challenge the process in court.[204] And indeed, several petitions for review asserted that one of the Order's legal defects was that it "conflicts with the notice-and-comment requirements of 5 U.S.C. § 553."[205] Strikingly, the briefs ultimately filed in these cases did *not* argue that there had been an APA violation.[206] When push came to shove a bunch of very good lawyers seem to have concluded that that was not a winning argument. I think they were right.

VI. MOVING FORWARD

Some negative recommendations flow from the foregoing. First, submitters of malattributed comments should not be prosecuted; they have not committed a crime. Second, regulations that emerge from a notice-and-comment process that included malattributed comments—even millions of them—should not be set aside for that reason; there is no harmful per se error in the comment process that requires a second go-round. Third, there is no reason an agency cannot read and be informed by a malattributed comment. It should give such comments, like all comments, the weight they deserve; that weight is a function of their

---

204 *See, e.g.*, Fung, *supra* note 59 (quoting Evan Greer of Fight for the Future as stating that "this will absolutely show up in court if we get there"); *see also* Karl Bode, *The FCC Is Blocking a Law Enforcement Investigation Into Net Neutrality Comment Fraud*, VICE (Dec. 12, 2017, 11:42 AM), https://www.vice.com/en_us/article/wjzjv9/net-neutrality-fraud-ny-attorney-general-investigation [https://perma.cc/87RP-DQAQ] ("Expect the agency's failure to police comment fraud to play a starring role in these legal arguments to come.").

205 Center for Democracy and Technology v. FCC, No. 18-1068 (D.C. Cir.), Petition for Review at 2 (Mar. 5, 2018); State of New York v. FCC, No. 18-1055 (D.C. Cir.), Petition for Review at 2 (Feb. 22, 2018).

206 Accordingly, the D.C. Circuit's opinion, which was largely but not entirely in the agency's favor, does not mention the "fraudulent comments" issue. *See* Mozilla Corp. v. FCC, 940 F.3d 1 (D.C. Cir. 2019).

content, not, in general, a function of the name of the submitter. It would not be reasoned decision-making for an agency to tally comments, malattributed or otherwise. But an agency can consider and rely on useful, relevant, accurate information or arguments from any source. Indeed, if it has not prohibited the submission of such comments (on which more below) it *must* consider such comments.

Nonetheless, malattributed comments do cause harms. The appropriate responses are not so much legal as technological. Tools that are commonplace in other settings where identity is important—notably online commercial or financial transactions—are adaptable to the rulemaking setting. Others with more expertise than I have recommended implementing CAPTCHA technology, adopting some sort of outside verification for comments, using two-step verification or confirmation email, or keeping track of and indicating the number of comments submitted from any individual email address.[207] All of these have meaningful shortcomings at present. But some effort by agencies and the General Services Administration to develop technological responses that make it harder to submit and easier to identify malattributed comments is appropriate. That work is already underway.[208]

Finally, agencies can reduce the incentive to file malattributed comments by refusing to consider them. To be sure, the APA requires agencies to consider "the relevant matter presented."[209] A strong reading of this provision would compel agencies to consider even malattributed comments—which "matter" and were "presented"—as long as their content is relevant to the rulemaking. However, on either of two theories an agency could refuse to consider malattributed comments.

First, an agency can set reasonable rules for which comments it will consider and which it will ignore. An agency can impose a deadline for comments, require submission to a particular address or website, prohibit use of profanity, and refuse to accept comments that contain confidential

---

207 *See* Singel, *supra* note 2; Weiss, *supra* note 167.

208 *See* U.S. General Services Administration, *Managing the Federal Rulemaking Process*, https://www.gsa.gov/policy-regulations/regulations/managing-the-federal-rulemaking-process [https://perma.cc/F43R-B28Q] (describing beta test of reCAPTCHA on regulations.gov as "part of ongoing efforts to support the integrity of the rulemaking process and manage the role of software-generated comments").

209 5 U.S.C. § 553(c) (2018).

business information.[210] Refusing to consider malattributed comments is no different. It leaves other channels open, imposes no burden or cost on authentic commenters, and is easily complied with. Indeed, if an agency can refuse to accept anonymous comments, which is undisputed, a fortiori it can refuse to accept malattributed comments.

The second theory rests on the text of § 553. An agency need only consider comments from "interested persons." No agency has ever read this language to limit the permissible range of commenters, and in ordinary circumstances it should not be read to do so. [211] However, an agency might conclude that someone who had no involvement at all in the submission of "their" comment is not an "interested person" and so the comment can be ignored. Of course, the *actual*, unnamed submitter *is* an "interested person;" so the question is whether the agency looks to the identity of the actual or the supposed submitter. Opting for the latter is inaccurate but can be defended as a reasonable administrative rule.

Refusing to consider malattributed comments will not eliminate them. First, agencies will not be able to identify all such comments, and submitters know it. Second, submitters may have audiences other than the agency—the press, the general public, legislators, a public relations firm's clients—and goals other than influencing agency policy (such as undermining public confidence in the regulatory process). But it would have some deterrent effect.

One other measure is appropriate. As discussed above, there are situations where the identity of the commenter does matter. Suppose, in the net neutrality rulemaking, a comment arrives that purports to be from the General Counsel of Verizon, but is not.[212] Or in a Department of Transportation rulemaking someone falsely submits a comment on the letterhead of General Motors or Ralph Nader. In general, the deception will be obvious and therefore inconsequential. But that will not always be the case, especially with less prominent figures. If the agency cares about

---

210 *See, e.g.*, Reytblatt v. U.S. Nuclear Reg. Comm'n, 105 F.3d 715, 723 (D.C. Cir. 1997) (holding that agency was not required to consider comments submitted after the agency-imposed deadline); Board of Regents of the Univ. of Wash. v. EPA, 86 F.3d 1214, 1222 (D.C. Cir. 1996) (same).

211 Michael Herz, *"Data, Views, or Arguments": A Rumination*, 22 WM. & MARY BILL OF RIGHTS J. 351, 357–59 (2013).

212 *See* Lapowsky, *supra* note 79 (describing the FiscalNote gravitas score and observing that "a comment's gravitas score would be higher if, say, it was written by Verizon's general counsel").

the source of the comment and has doubts, there is an easy step it can take: *ask*. But suppose it is wholly duped, and so does not think to ask. It has one other resource: scrutiny of comments for malattribution can be crowdsourced by outside stakeholders who monitor the docket. For this to be most effective, the agency should do two things. First, it should post comments to regulations.gov in a timely manner. If the comments are not available, they cannot be monitored. Second, it should use a reply period. Reply periods in notice-and-comment rulemaking are unusual, though some agencies—including, notably, the FCC—do provide them. Their potential value is obvious; they also can be messy and create an incentive for commenters to hold back their main points during the "regular" comment period and only release them during the reply period so they cannot be rebutted. ACUS has stopped shy of calling for reply periods across the board but has endorsed their use as appropriate.[213] One benefit of a reply period is that it would allow the agency to crowdsource identification of malattributed comments. The Verizon General Counsel can easily check the docket for phony submissions in her name and inform the agency. Indeed, this can happen even without a formal reply period.

Finally, former FCC Commissioner Harold Furchtgott-Roth argues for a simple deterrent to mass comments in all their forms: a commenting fee.[214] He suggests 49 cents. It is a classic economist's response; a good (agencies' time, attention, and docket space) is being wasted, so charge for it. The charge would duplicate the pre-online system, where commenters had to bring the comment in person (which had a cost) or

---

213 *See* Administrative Conference of the United States, Rec. No. 2011-2, *Rulemaking Comments* ¶ 6 (2011) ("Where appropriate, agencies should make use of reply comment periods or other opportunities for receiving public input on submitted comments, after all comments have been posted."); Administrative Conference of the United States, Rec. No. 76-3, *Procedures in Addition to Notice & the Opportunity for Comment in Informal Rulemaking* (1976) (recommending a second comment period in proceedings in which comments or the agency's responses thereto "present new and important issues or serious conflicts of data"); Administrative Conference of the United States, Rec. No. 72-5, *Procedures for the Adoption of Rules of General Applicability* (1972) (recommending that agencies consider providing an "opportunity for parties to comment on each other's written or oral submissions.").

214 Harold Furchtgott-Roth, *How to Reduce Frivolous Comments in Federal Proceedings*, FORBES (July 21, 2017, 12:59 PM), https://www.forbes.com/sites/haroldfurchtgottroth/2017/07/21/how-to-reduce-frivolous-comments-in-federal-proceedings/#18373a5e3e70 [https://perma.cc/4BLL-2SYX].

pay postage. And it would likely have a meaningful impact on bot-generated comments, malattributed or not, without being a significant burden on those submitting just one comment. Nonetheless, it is a bad idea for reasons both real and symbolic. It is arguably inconsistent with both the APA and the E-Government Act and would almost certainly require legislative authorization even were it not. More important, rules that make it easier for well-funded or corporate and institutional commenters to participate than individuals, small businesses, and non-profits are virtually always a mistake, even if the burden is slight. They will have a disparate impact on who does participate and send a message that the agency is just fine with such an outcome.

CONCLUSION

In the early days of electronic rulemaking, Beth Noveck celebrated the benefits of lay participation in rulemaking: "Participation sharpens democratic skills, instills a sense of civic responsibility, and deepens democratic political culture. By cultivating participation in this domain, participation reinforces democratic practice throughout civic life and cultivates the moral imperative as well as the general will."[215] It is a happy picture. It is also the complete opposite of, and mocked by, malattributed, computer-generated comments filed over the names of individuals who had nothing to do with the submission and may fundamentally disagree with it. There is nothing to celebrate about such comments. Agencies should make reasonable efforts to prevent, minimize, and silo them. But they are not illegal, and they are not a cataclysm. They are pink eye.

215 *See* Beth Simone Noveck, *The Electronic Revolution in Rulemaking*, 53 EMORY L.J. 433, 460 (2004).