

Copyright 2020 by Michael A. Cheah  
Northwestern University Law Review

Vol. 115

## SECTION 230 AND THE TWITTER PRESIDENCY

*Michael A. Cheah*

**ABSTRACT**—In response to Twitter’s decision to label one of the President’s tweets misleading, the Trump White House issued an executive order to limit the scope of Section 230 of the Communications Decency Act via agency rulemaking. In the Order, Trump calls for the Federal Communications Commission (FCC) to “interpret” Section 230 in a manner that curtails websites’ ability to remove and restrict user speech. This Essay analyzes the Order and concludes that the President’s effort to limit Section 230 will fail. First, the FCC does not have rulemaking authority to issue the proposed rules. Second, the proposed rules cannot be issued because they are inconsistent with the statute. Finally, this Essay will discuss the policy implications of the proposed rules and argue that they would lead to less speech and engagement on the Internet, not more of it.

**AUTHOR**—General Counsel of Vimeo, Inc. and adjunct faculty at the University of Miami School of Law. A big thank you to my colleague Erika Barros Sierra Cordera at Vimeo for help in researching and editing, Professor Caroline Mala Corbin at the University of Miami School of Law for her excellent feedback, and the *Northwestern University Law Review* for their diligent and timely work in shepherding this Essay to publication.

INTRODUCTION .....	193
I. SECTION 230 OF THE COMMUNICATIONS DECENCY ACT .....	196
A. <i>The Genesis of Section 230</i> .....	196
B. <i>Judicial Interpretation of Section 230</i> .....	198
II. THE FCC LACKS AUTHORITY TO ENGAGE IN THE PROPOSED RULEMAKING .....	204
A. <i>Proposed Rules Under the Executive Order and NTIA Petition</i> .....	204
B. <i>FCC Rulemaking Authority Under the Communications Act</i> .....	206
C. <i>NTIA’s Attempt to Find Rulemaking Authority Under the Common         Carrier Provisions of the Communications Act</i> .....	209
D. <i>The FCC’s Lack of Rulemaking Authority Under Section 230</i> .....	210
III. THE PROPOSED RULES ARE INCONSISTENT WITH SECTION 230 .....	211
A. <i>The Proposed Limitation of Section 230(c)(1)</i> .....	211
B. <i>The Proposed Restriction of Section 230(c)(2)</i> .....	213
C. <i>The Proposed Introduction of an Objective Standard</i> .....	214
D. <i>The Proposed Due Process Requirements</i> .....	214
IV. POLICY CONSIDERATIONS .....	216
A. <i>Increased Moderation Challenges</i> .....	216
B. <i>More Harmful Speech Online</i> .....	219
C. <i>An Illusory Immunity</i> .....	221
CONCLUSION.....	222

## INTRODUCTION

It was years in the making, but on May 26, 2020, Twitter finally<sup>1</sup> took action on the account of @realDonaldTrump.<sup>2</sup> As content moderation goes, the action was fairly modest. Twitter appended the following to a tweet making misleading claims about mail-in voting: “Get the facts about mail-in ballots”<sup>3</sup> and a link to accurate voting information.<sup>4</sup> The President’s response was swift and retributive. Within hours, he tweeted that Twitter is “now interfering in the 2020 Presidential Election” and “completely stifling FREE

<sup>1</sup> Elizabeth Dwoskin, *Twitter’s Decision to Label Trump’s Tweets Was Two Years in the Making*, WASH. POST (May 29, 2020, 6:55 PM), <https://www.washingtonpost.com/technology/2020/05/29/inside-twitter-trump-label/> [https://perma.cc/6FWD-HR5D].

<sup>2</sup> Donald J. Trump (@realDonaldTrump), TWITTER, <https://twitter.com/realDonaldTrump> (last visited Oct. 26, 2020).

<sup>3</sup> Donald J. Trump (@realDonaldTrump), TWITTER (May 26, 2020, 7:17 AM), <https://twitter.com/realDonaldTrump/status/1265255845358645254> [https://perma.cc/9DRW-2L7N].

<sup>4</sup> See *Trump Makes Unsubstantiated Claim That Mail-In Ballots Will Lead to Voter Fraud*, TWITTER (May 26, 2020), <https://twitter.com/i/events/1265330601034256384> [https://perma.cc/NC44-2P9B].

SPEECH.”<sup>5</sup> And within two days, he signed Executive Order 13,925, titled “Preventing Online Censorship,”<sup>6</sup> a proclamation that seeks to punish large social media platforms that have the temerity to fact-check the President.<sup>7</sup>

The Executive Order represents an effort to undermine the immunity that platforms like Twitter and Facebook enjoy under Section 230 of the Communications Decency Act (CDA) when it comes to moderating user content<sup>8</sup>—Section 230 grants broad immunity to websites with respect to decisions they make about publishing and removing user content.<sup>9</sup> The Executive Order directs the Commerce Department to file a rulemaking petition before the Federal Communications Commission (FCC) to “clarify” the existing immunity, by which the Order really means to rewrite the statute in the guise of making it clearer.<sup>10</sup>

As explained in this Essay, this convoluted attempt to bypass Congress will not succeed. Yet, it would be a mistake to ignore the Order as it comes at a time when there is vigorous public debate over the scope of Section 230 and platforms’ social responsibilities in general.<sup>11</sup> There are essentially two debates about Section 230 occurring simultaneously and at cross purposes: conservatives see liberal bias against conservative speech and seek to constrain service providers’ discretion in removing content, while the other side of the aisle sees too little action over hate speech, fake news, and other problematic content and seeks obligations to remove such content.<sup>12</sup> As Internet law scholar Professor Eric Goldman puts it, “Section 230 is a magnet

---

<sup>5</sup> Donald J. Trump (@realDonaldTrump), TWITTER (May 26, 2020, 6:40 PM), <https://twitter.com/realDonaldTrump/status/1265427538140188676> [<https://perma.cc/V2MF-DFBL>].

<sup>6</sup> Exec. Order No. 13,925, 85 Fed. Reg. 34,079 (June 2, 2020), <https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/> [<https://perma.cc/EY88-EGAK>].

<sup>7</sup> For this reason, one organization has challenged the Order on First Amendment grounds. *See* Complaint at ¶¶ 9–12, *Ctr. for Democracy & Tech. v. Trump*, No. 20-1456 (D.D.C. June 2, 2020).

<sup>8</sup> *See* Exec. Order No. 13,925, 85 Fed. Reg. 34,079 at 34,080–81.

<sup>9</sup> 47 U.S.C. §§ 230(c)(1), (c)(2); *Force v. Facebook, Inc.*, 934 F.3d 53, 64 (2d Cir. 2019) (citations omitted) (“In light of Congress’s objectives, the Circuits are in general agreement that the text of Section 230(c)(1) should be construed broadly in favor of immunity.”).

<sup>10</sup> Exec. Order No. 13,925, 85 Fed. Reg. 34,079 at 34,081.

<sup>11</sup> *See* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1652–57 (2018) (describing negative publicity over high-profile content moderation incidents and pressures on platforms to moderate offensive content); *see also* John Samples, *Why the Government Should Not Regulate Content Moderation of Social Media*, 865 POL’Y ANALYSIS 1, 1–2 (2019) (describing criticism of platforms’ moderation decisions).

<sup>12</sup> *See* PAUL M. BARRETT, REGULATING SOCIAL MEDIA: THE FIGHT OVER SECTION 230—AND BEYOND 2–3 (2020), [https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/5f4d682af956e403bdd2dcf5/1598908459863/NYU+Section+230\\_FINAL+ONLINE+UPDATED\\_Aug+26.pdf](https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/5f4d682af956e403bdd2dcf5/1598908459863/NYU+Section+230_FINAL+ONLINE+UPDATED_Aug+26.pdf) [<https://perma.cc/MH2J-8AJZ>].

for controversy, and this order pours fuel on the fire.”<sup>13</sup> Indeed, the Order has spawned proposed legislation that would implement its principal proposed limitations on the scope of Section 230.<sup>14</sup>

Part I of this Essay reviews the genesis of Section 230 and the immunity it confers. Part II then discusses the Executive Order’s proposed rules and analyzes whether the FCC has the authority to promulgate rules under Section 230, concluding that it does not. The Executive Order seeks to constrain websites’ discretion to remove content by requiring them to provide users with certain aspects of procedural due process, such as notice, reasoned decisions, and the opportunity to be heard.<sup>15</sup> Yet, nothing in the FCC’s authorizing statute, the Communications Act of 1934,<sup>16</sup> expressly grants the FCC authority to regulate Internet content, and Section 230 gives the FCC no role to play. While there are some additional potential sources of authority available, the FCC, currently led by Trump appointees, has closed off these avenues.

Part III examines whether the FCC could issue the Executive Order’s proposed rules even if it had authority. It concludes that the FCC cannot because there is no ambiguity in the statute permitting the proposed interpretations, and, moreover, the interpretations are inconsistent with the text of Section 230.

Lastly, Part IV reviews the policy implications of the proposed due process rules on content moderation. It concludes that instead of increasing free speech, the rules will have the opposite effect and will lead to more unwanted speech and less civil engagement online.

---

<sup>13</sup> Peter Baker & Daisuke Wakabayashi, *Trump’s Order on Social Media Could Harm One Person in Particular: Donald Trump*, N.Y. TIMES (May 28, 2020), <https://www.nytimes.com/2020/05/28/us/politics/trump-jack-dorsey.html> [<https://perma.cc/Y5DU-VFGK>] (quoting Professor Eric Goldman).

<sup>14</sup> On September 8, 2020, Senators Roger Wicker (R-MS), Lindsay Graham (R-SC), and Marsha Blackburn (R-TN) introduced a bill titled the Online Freedom and Viewpoint Diversity Act. A copy of the bill, unnumbered as of this date, is available at <https://www.commerce.senate.gov/services/files/94D0F3C6-B927-46D2-A75C-17C78D0D92AA> [<https://perma.cc/8F28-VSYK>]. The bill adopts a number of the Executive Order’s proposals. And before the Executive Order, Senators Brian Schatz (D-HI) and John Thune (R-SD) introduced the also unnumbered Platform Accountability and Consumer Transparency Act, <https://www.schatz.senate.gov/imo/media/doc/OLL20612.pdf> [<https://perma.cc/8ZNV-5KFH>], which would, among other things, require service providers to give users the right to appeal decisions by the service providers to remove their content.

<sup>15</sup> Exec. Order No. 13,925, 85 Fed. Reg. 34,079 at 34,081.

<sup>16</sup> Codified at 47 U.S.C. § 151.

## I. SECTION 230 OF THE COMMUNICATIONS DECENCY ACT

Passed as the Cox-Wyden Amendment to the Telecommunications Act of 1996,<sup>17</sup> Section 230 of the CDA<sup>18</sup> is often cited as the most important piece of legislation governing the Internet as it gives websites and other online services freedom to make vast quantities of user content available without worrying that any single piece of content might be tortious or illegal.<sup>19</sup> The central idea behind the statute is that websites should not be held liable for the decisions they make as to whether to publish or withdraw user content, and that they should be encouraged in their efforts to remove user content.<sup>20</sup> Section 230 accomplishes this by providing users and service providers with affirmative defenses<sup>21</sup> to civil<sup>22</sup> and certain criminal liability<sup>23</sup> under state<sup>24</sup> and federal laws.<sup>25</sup>

A. *The Genesis of Section 230*

Section 230 was passed in response to a pair of trial court decisions in the mid-1990s that gave members of Congress pause.<sup>26</sup> The first case, *Cubby*,

---

<sup>17</sup> Pub. L. No. 104-104, § 509, 110 Stat. 56, 137–39 (1996) (codified at 47 U.S.C. § 230). Title V of the Act is called the Communications Decency Act.

<sup>18</sup> 47 U.S.C. § 230 (2018).

<sup>19</sup> As explained by preeminent First Amendment scholar and Internet policy expert Marvin Ammori, Section 230 does for online publishers what *New York Times Co. v. Sullivan* did for print newspapers. Marvin Ammori, *The “New” New York Times: Free Speech Lawyering in the Age of Google and Twitter*, 127 HARV. L. REV. 2259, 2263–64 (2014). In *New York Times Co. v. Sullivan*, the Supreme Court held that First Amendment principles required that the tort of defamation be altered such that when the plaintiff is a public figure, the plaintiff must prove “actual malice.” 376 U.S. 254, 279–80 (1964). This gives speakers, including newspapers and other publishers, more freedom to report upon and criticize public figures. Ammori argues that Section 230 provides online services with similar breathing room. Ammori, *supra*, at 2263–64.

<sup>20</sup> See, e.g., *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1170–71 (9th Cir. 2008) (en banc) (explaining that “section 230 was meant to provide immunity [such that] any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230”).

<sup>21</sup> See *Klayman v. Zuckerberg*, 753 F.3d 1354, 1357 (D.C. Cir. 2014).

<sup>22</sup> See 47 U.S.C. § 230(c)(2) (heading referring to “civil liability”).

<sup>23</sup> All inconsistent state laws are expressly preempted. *Id.* § 230(e)(3). Federal criminal laws are specifically excluded from Section 230’s ambit. *Id.* § 230(e)(1); see also *Doe v. Backpage.com, LLC*, No. 17-11069, 2018 WL 1542056, at \*2 (D. Mass. Mar. 29, 2018) (explaining that Section 230 “creat[es] immunity from civil and state criminal law, but not federal criminal law”). Following a 2018 amendment, Congress carved out state criminal prosecutions for sex trafficking and prostitution. See 47 U.S.C. § 230(e)(5)(B)–(C).

<sup>24</sup> 47 U.S.C. § 230(e)(3).

<sup>25</sup> For example, Section 230 applies to later-enacted federal laws. See *Doe v. Backpage.com, LLC*, 817 F.3d 12, 15, 23 (1st Cir. 2016) (finding that Section 230(e)(1) precluded civil liability under Trafficking Victims Protection Reauthorization Act of 2008), *abrogated by statute*, 47 U.S.C. § 230(e)(5).

<sup>26</sup> 141 CONG. REC. H8469–70 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

*Inc. v. CompuServe, Inc.*, concluded that CompuServe, an early online service, could not be held liable for defamation based upon user content unless it had actual notice of defamation.<sup>27</sup> The court reasoned that CompuServe resembled a “distributor” under common law tort principles akin to a bookstore or newsstand because it did not screen user content.<sup>28</sup> Just as newsstands and bookstores are not liable for selling defamatory newspapers and books (unless they have reason to know about the defamatory statements), nor should CompuServe be liable for the user’s defamation.<sup>29</sup> The second case, *Stratton Oakmont, Inc. v. Prodigy Services Co.*, involved Prodigy, a provider that screened for content unsuitable for children.<sup>30</sup> Having undertaken screening efforts, the court ruled that Prodigy should be treated as a publisher—like a news editor—rather than a distributor, and thus should face liability for defamatory user content, even in the absence of notice or actual knowledge.<sup>31</sup>

Congress recognized that this liability regime would, perversely, penalize good Samaritans like the family-friendly Prodigy.<sup>32</sup> As Professor Goldman explains, *Stratton Oakmont* created the “moderator’s dilemma”: service providers must choose between aggressively removing content or curtailing moderation activities so that they do not put themselves on notice of potential illegality.<sup>33</sup> Both options are unpalatable: the former reduces speech while the latter results in the proliferation of unsuitable content online.<sup>34</sup>

To remove the disincentives for self-regulation, Section 230 overrules *Stratton Oakmont*, immunizing website operators with respect to certain

<sup>27</sup> 776 F. Supp. 135, 140–41 (S.D.N.Y. 1991). Under New York law, for example, “vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation.” *Id.* at 139 (quoting *Lerman v. Chuckleberry Publ’g, Inc.*, 521 F. Supp. 228, 235 (S.D.N.Y. 1981)).

<sup>28</sup> *Id.* at 140–41.

<sup>29</sup> This common law rule is “deeply rooted in the First Amendment” concern that if a bookseller had to make himself aware of the contents of every book in his shop, such an unreasonable burden would “become the public’s burden, for by restricting him the public’s access to reading matter would be restricted.” *Id.* at 139–40 (quoting *Smith v. California*, 361 U.S. 147, 153 (1959)).

<sup>30</sup> No. 31063/94, 1995 WL 323710, at \*4–5 (N.Y. Sup. Ct. May 24, 1995).

<sup>31</sup> *Id.*

<sup>32</sup> 141 CONG. REC. H8469–70 (daily ed. Aug. 4, 1995) (statement of Rep. Cox) (describing the outcomes of *Stratton Oakmont* as “backward” in the context of *Cubby, Inc.*); see also *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 173 (2d Cir. 2016) (explaining that “[t]he [CDA] was intended to overrule *Stratton [Oakmont]* and provide immunity for ‘interactive computer service[s]’ that make ‘good faith’ efforts to block and screen offensive content”).

<sup>33</sup> Eric Goldman, *An Overview of the United States’ Section 230 Internet Immunity*, in *THE OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY 3* (Giancarlo Frosio ed., 2020).

<sup>34</sup> See *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997).

decisions they make concerning user-generated content.<sup>35</sup> Under the heading “Protection for ‘Good Samaritan’ blocking and screening of offensive material,”<sup>36</sup> Section 230(c) immunizes service providers from (1) actions undertaken as a publisher;<sup>37</sup> and (2) good faith efforts to remove or restrict offensive content.<sup>38</sup> Subject to certain exemptions (such as federal criminal prosecutions and intellectual property laws),<sup>39</sup> these immunities modify other federal laws<sup>40</sup> and preempt inconsistent state laws.<sup>41</sup> It thus acts as a type of “super statute.”<sup>42</sup>

Congress also took the “rather unusual step”<sup>43</sup> of announcing its policy objectives in Section 230(b), which states that Congress’s objectives are to, *inter alia*, “preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;”<sup>44</sup> “encourage the development of technologies [that] maximize user control” about what individuals, families, and schools see;<sup>45</sup> and “remove disincentives for the development and utilization of blocking and filtering technologies [to] empower parents to restrict their children’s access to objectionable or inappropriate online material.”<sup>46</sup>

### *B. Judicial Interpretation of Section 230*

Guided by Congress’s express goals, courts have established a robust body of law interpreting Section 230 broadly in favor of immunity for

---

<sup>35</sup> 47 U.S.C. § 230(c) (2018).

<sup>36</sup> *Id.*

<sup>37</sup> *Id.* § 230(c)(1).

<sup>38</sup> *Id.* § 230(c)(2)(A).

<sup>39</sup> *Id.* § 230(e)(1), (2), (4).

<sup>40</sup> See *Force v. Facebook, Inc.*, 934 F.3d 53, 71–72 (2d Cir. 2019) (applying Section 230 to civil claim under federal anti-terrorism law).

<sup>41</sup> 47 U.S.C. § 230(e)(3).

<sup>42</sup> See *Bostock v. Clayton Cnty.*, 140 S. Ct. 1731, 1754 (2020) (describing the federal Religious Freedom Restoration Act as a “super statute” because it “displac[es] the normal operation of other federal laws”).

<sup>43</sup> *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1047 (9th Cir. 2019), *cert. denied*, No. 19-1284, 2020 WL 6067214, at \*1 (Oct. 13, 2020). Legislative statements by Section 230’s sponsors indicate that this statement of policy was intended to ward off federal regulation of Internet content. See 141 CONG. REC. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Cox) (“[I]t will establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet . . .”).

<sup>44</sup> 47 U.S.C. § 230(b)(2).

<sup>45</sup> *Id.* § 230(b)(3).

<sup>46</sup> *Id.* § 230(b)(4).

websites and other online services that host user content.<sup>47</sup> Although the Supreme Court has reviewed unrelated provisions of the CDA,<sup>48</sup> it has not yet reviewed a case involving Section 230.<sup>49</sup> As such, this Essay will briefly review some of the key lower court decisions.

The “typical” Section 230 case involves a situation where a service provider has published allegedly illegal user content.<sup>50</sup> A smaller, but increasingly litigated, category involves challenges of content removal decisions.<sup>51</sup> Service providers have generally been successful in suppressing both categories of claims based upon Section 230(c)(1), which states that service providers shall not be considered publishers or speakers of content posted by others.<sup>52</sup> In addition to this provision, Section 230(c)(2) provides for immunity for service providers who voluntarily remove or restrict access to certain types of objectionable content,<sup>53</sup> and thus more directly addresses the act of content removal.<sup>54</sup>

### 1. Section 230(c)(1)

Section 230(c)(1) states that no service provider “shall be treated as the publisher or speaker of any information provided by another information content provider.”<sup>55</sup> No discussion of this language is complete without mentioning the Fourth Circuit’s 1997 decision in *Zeran v. American Online*.<sup>56</sup> There, a defamation plaintiff asserted that Section 230 did not bar his claims because the service provider had notice of the defamatory user content.<sup>57</sup> In his view, Congress, by using the term “publisher” in Section

<sup>47</sup> *Force v. Facebook, Inc.*, 934 F.3d 53, 64 (2d Cir. 2019) (“In light of Congress’s objectives, the Circuits are in general agreement that the text of Section 230(c)(1) should be construed broadly in favor of immunity.”).

<sup>48</sup> *Reno v. ACLU*, 521 U.S. 844, 849, 882 (1997) (striking down on First Amendment grounds anti-indecency provisions of the Communications Decency Act, previously codified as 47 U.S.C. § 223).

<sup>49</sup> *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, No. 19-1284, 2020 WL 6067214, at \*1 (Oct. 13, 2020) (explaining that “in the 24 years since [its passage], we have never interpreted this provision”) (Thomas, J., in respect of denial of certiorari). Justice Thomas recently questioned lower courts’ broad interpretations of Section 230, *see id.*, and suggested that, “in an appropriate case, we should consider whether the text of this increasingly important statute aligns with the current state of immunity enjoyed by Internet platforms.” *Id.*

<sup>50</sup> *Domen v. Vimeo, Inc.*, 433 F. Supp. 3d 592, 602 (S.D.N.Y. 2020) (“In the typical case, plaintiffs seek to hold the interactive computer service liable for publishing the content of a third party . . . and immunity from liability under (c)(1) is found in that context.”).

<sup>51</sup> *See id.*

<sup>52</sup> 47 U.S.C. § 230(c)(1).

<sup>53</sup> *Id.* § 230(c)(2).

<sup>54</sup> *Force v. Facebook, Inc.*, 934 F.3d 53, 64 n.16 (2d Cir. 2019) (observing that Section 230(c)(2) “responds to *Stratton [Oakmont]* even more directly”).

<sup>55</sup> 47 U.S.C. § 230(c)(1).

<sup>56</sup> 129 F.3d 327, 328 (4th Cir. 1997).

<sup>57</sup> *Id.* at 329, 331.



230(c)(1), meant only to abrogate *Stratton Oakmont*, while preserving the “distributor,” or notice-based, liability as set forth in *Cubby*.<sup>58</sup>

The Fourth Circuit rejected this approach, finding that notice-based liability would, like *Stratton Oakmont* itself, “reinforce[] service providers’ incentives to restrict speech [or] abstain from self-regulation.”<sup>59</sup> First, the court reasoned that requiring “on-the-spot editorial decision[s]” upon notice would not be feasible given “the sheer number of postings on interactive computer services.”<sup>60</sup> And because providers would face liability only for content they did not remove, there would be “a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not,” thus chilling speech.<sup>61</sup> Second, some providers would actively avoid moderation activities because “efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability.”<sup>62</sup>

Today, federal and state courts<sup>63</sup> agree that Section 230(c)(1) applies whenever three things are true: (1) the defendant provides an “interactive computer service;” (2) the defendant did not create the “information content” at issue; and (3) the plaintiff’s claims “seek[] to hold a service provider liable for its exercise of a publisher’s traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content.”<sup>64</sup> Put another way, “any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230.”<sup>65</sup>

Early Section 230 cases involved plaintiffs asserting claims of defamation against service providers based upon libelous user postings.<sup>66</sup>

---

<sup>58</sup> *Id.* at 331–32.

<sup>59</sup> *Id.* at 333.

<sup>60</sup> *Id.*

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

<sup>63</sup> *See, e.g.*, *Force v. Facebook, Inc.*, 934 F.3d 53, 64 (2d Cir. 2019) (“In light of Congress’s objectives, the Circuits are in general agreement that the text of Section 230(c)(1) should be construed broadly in favor of immunity.”); *Shiamili v. Real Est. Grp. of N.Y., Inc.*, 952 N.E.2d 1011, 1016(N.Y. 2011) (explaining that “[b]oth state and federal courts around the country have ‘generally interpreted Section 230 immunity broadly’”); *Barrett v. Rosenthal*, 146 P.3d 510, 513 (Cal. 2006) (“These provisions have been widely and consistently interpreted to confer broad immunity against defamation liability for those who use the Internet to publish information that originated from another source.”).

<sup>64</sup> *Zeran*, 129 F.3d at 330; *see also, e.g.*, *Jones v. Dirty World Entm’t Recordings LLC*, 755 F.3d 398, 407–09 (6th Cir. 2014) (adopting *Zeran* formulation); *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 174 (2d Cir. 2016) (applying *Zeran* framework).

<sup>65</sup> *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1170–71 (9th Cir. 2008) (en banc).

<sup>66</sup> *See, e.g.*, *Zeran*, 129 F.3d at 330.

Subsequent cases have extended Section 230 beyond defamation to claims ranging from negligence resulting in offline harm<sup>67</sup> to civil causes of action under federal anti-terrorism laws.<sup>68</sup>

Section 230(c)(1) is not, however, without limitation. By its terms, the statute does not apply to content created by the website itself.<sup>69</sup> Thus, a service provider's own speech online is never immune from liability.<sup>70</sup> Nor can a provider avoid liability where it contributed materially to the illegality of the challenged content.<sup>71</sup> Finally, Section 230(c)(1) does not apply where liability stems from a website's act that is independent of its publishing choices.<sup>72</sup>

## 2. Section 230(c)(2)

Section 230(c)(2) contains two parts. Section 230(c)(2)(A) states that no service provider shall be liable for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."<sup>73</sup> This immunity applies when the defendant: (1) removed or restricted access to online materials; (2) acted in good faith; and (3) considered the materials to fall into one of the covered categories.

Although this first part of this provision more directly responds to *Stratton Oakmont* and Congress's concerns about disincentives to remove content,<sup>74</sup> it has been less frequently litigated.<sup>75</sup> And much of that litigation has focused on the scope of the catch-all term "otherwise objectionable."<sup>76</sup> Some district courts have held that the term is not completely open-ended and must bear some relationship with the enumerated terms under the canon

<sup>67</sup> See *Doe v. MySpace, Inc.*, 528 F.3d 413, 413 (5th Cir. 2008).

<sup>68</sup> See *Force*, 934 F.3d at 53.

<sup>69</sup> *Zeran*, 129 F.3d at 330 ("None of this means, of course, that the original culpable party who posts defamatory messages would escape accountability.").

<sup>70</sup> See *id.* at 330–31.

<sup>71</sup> *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1170–71 (9th Cir. 2008) (en banc).

<sup>72</sup> See *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1102 (9th Cir. 2009).

<sup>73</sup> 47 U.S.C. § 230(c)(2)(A).

<sup>74</sup> *Force v. Facebook, Inc.*, 934 F.3d 53, 80 (2d Cir. 2019) (Katzmann, C.J., concurring in part and dissenting in part).

<sup>75</sup> Eric Goldman, *Why Section 230 Is Better than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33, 40 (2019).

<sup>76</sup> See *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1049 (9th Cir. 2019) (observing that "[d]istrict courts nationwide have grappled with the issues" presented by this term), *cert. denied*, No. 19-1284, 2020 WL 6067214, at \*1 (Oct. 13, 2020).

*ejusdem generis*,<sup>77</sup> the principle that “when a general term follows a specific one, the general term should be understood as a reference to subjects akin to the one with specific enumeration.”<sup>78</sup> The only appellate decision on this score has rejected that view. In *Enigma Software v. Malwarebytes*, the Ninth Circuit concluded that *ejusdem generis* supplied little assistance because the enumerated categories lacked commonality, explaining that “[m]aterial that is lewd or lascivious is not necessarily similar to material that is violent, or material that is harassing.”<sup>79</sup> Accordingly, because the enumerated terms “vary greatly . . . the catchall was more likely intended to encapsulate forms of unwanted online content that Congress could not identify in the 1990s.”<sup>80</sup>

The second part of this provision, 230(c)(2)(B), is an immunity that allows “any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in” the first paragraph (i.e., the enumerated categories and “otherwise objectionable” content).<sup>81</sup> This immunity allows users and service providers to develop tools that allow others to restrict and remove materials, such as a tool that allows users to block or limit other users from commenting on their pages.<sup>82</sup>

### 3. Application to Users

Section 230(c)’s immunities do not just protect large social media platforms, they also protect “users” and any “providers” of interactive computer services.<sup>83</sup> While Section 230(c)(1) certainly immunizes Twitter from liability for a user’s defamatory tweet, it also protects the individuals who retweet it.<sup>84</sup> Thus, although President Trump may be upset about Twitter’s action as it relates to his mail-in-vote tweet<sup>85</sup> (an action that is,

---

<sup>77</sup> See, e.g., *Song Fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 883 (N.D. Cal. 2015); *Holomaxx Tech. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1104–05 (N.D. Cal. 2011).

<sup>78</sup> *Ali v. Fed. Bureau of Prisons*, 552 U.S. 214, 223 (2008) (quoting *Norfolk & Western R. Co. v. Am. Train Dispatchers Ass’n*, 499 U.S. 117, 129 (1991)).

<sup>79</sup> 946 F.3d at 1051.

<sup>80</sup> *Id.* at 1051–52.

<sup>81</sup> 47 U.S.C. § 230(c)(2). Technically, this provision ends with the words, “the material described in paragraph (1).” *Id.* Since there is no “paragraph (1),” this is a “typographical error,” as recognized by the United States Code Annotated. See 47 U.S.C.A. § 230(c)(2)(B) (West 2018).

<sup>82</sup> *Fehrenbach v. Zeldin*, No. 17-CV-5282, 2018 WL 4242452, at \*5 (E.D.N.Y. Aug. 6, 2018) (finding that section 230(c)(2)(B) precluded a lawsuit that “charges the Facebook defendants with enabling users to restrict access to material”).

<sup>83</sup> 47 U.S.C. §§ 230(c)(1), (2).

<sup>84</sup> See *Barrett v. Rosenthal*, 146 P.3d 510, 528–29 (2006) (concluding that “user” includes a user who knowingly republishes a defamatory post of another).

<sup>85</sup> See *supra* notes 1–5 and accompanying text. Twitter’s fact-check label would not be protected by Section 230 because it is “information content” created or developed by Twitter itself, not of “another information content provider.” *Id.*

ironically, not protected by Section 230), he enjoys Section 230 protection anytime he retweets content that may contain defamatory statements.<sup>86</sup> Indeed, part of what makes Section 230 so controversial is that this immunity applies even where the retweeting individual does so with knowledge that the content is defamatory since there is no good faith requirement in Section 230(c)(1).<sup>87</sup>

Section 230(c)(2) also protects each user's ability to block other users from reading and participating in their feeds.<sup>88</sup> This allows people to use their favorite social media apps without being subjected to harassment. Twitter recently launched a tool that allows people to determine who may reply to their tweets.<sup>89</sup> Indeed, before being ordered not to do so based upon the First Amendment, President Trump routinely blocked "persons expressing viewpoints he [found] distasteful" from his Twitter feed.<sup>90</sup> After President Trump returns to the private sector, he will presumably want to resume blocking individuals, an action protected by Section 230(c)(2).

#### 4. *Litigation of the Immunities in Practice*

Because the Section 230 immunities are affirmative defenses to liability,<sup>91</sup> the defendant service provider bears the burden of proof.<sup>92</sup> Still, Section 230 cases can be decided on motions to dismiss when the defense is evident from the complaint.<sup>93</sup> Because defendants do not need to prove any particular state of mind or that they took any affirmative steps, the Section 230(c)(1) immunity typically presents a question of law that can be resolved on a motion to dismiss,<sup>94</sup> thus "provid[ing] . . . legal certainty at a relatively low cost."<sup>95</sup>

---

<sup>86</sup> Baker & Wakabayashi, *supra* note 13.

<sup>87</sup> See *Barrett*, 146 P.3d at 529 ("The prospect of blanket immunity for those who intentionally redistribute defamatory statements on the Internet has disturbing implications").

<sup>88</sup> For an overview of Twitter functionality in a First Amendment context, see *Knight First Am. Inst. v. Trump*, 928 F.3d 226, 230–31 (2d Cir. 2019).

<sup>89</sup> Aja Romano, *Twitter Now Lets You Disable Replies. It Could Be Its Best Change Yet.*, VOX (May 27, 2020, 2:40 PM), <https://www.vox.com/2020/5/27/21265271/twitter-moderate-turn-off-replies-feature> [<https://perma.cc/L4RJ-XTHY>] (explaining that the "tool won't completely wipe out Twitter harassment, but it may drastically reduce it").

<sup>90</sup> *Knight First Am. Inst.*, 928 F.3d at 239. The court found that Trump's Twitter feed was a public forum claim under the First Amendment. *Id.* at 238.

<sup>91</sup> See *Klayman v. Zuckerberg*, 753 F.3d 1354, 1357 (D.C. Cir. 2014).

<sup>92</sup> See *Meacham v. Knolls Atomic Power Lab'y*, 554 U.S. 84, 91 (2008) (discussing affirmative defenses to find that "[w]hen a proviso . . . carves an exception out of the body of a statute or contract those who set up such exception must prove it") (alteration and omission in original) (quoting *Javierre v. Cent. Altigracia*, 217 U.S. 502, 508 (1910)).

<sup>93</sup> *Klayman*, 753 F.3d at 1357.

<sup>94</sup> See *Force v. Facebook, Inc.*, 934 F.3d 53, 63 n.15 (2d Cir. 2019).

<sup>95</sup> *Goldman*, *supra* note 75, at 42.

Because it contains a mental element (good faith),<sup>96</sup> Section 230(c)(2) may make somewhat of a less attractive case for a motion to dismiss as it could require discovery and even a trial where there is a genuine dispute over the defendant's state of mind. For this reason, Professor Goldman suspects that Section 230(c)(2) imposes "higher litigation burdens [which] discourage defendants from relying upon it."<sup>97</sup> Still, Section 230(c)(2) has been applied on motions to dismiss<sup>98</sup> and so it is not necessarily clear whether this is empirically the case.

## II. THE FCC LACKS AUTHORITY TO ENGAGE IN THE PROPOSED RULEMAKING

The FCC has many regulatory powers over interstate communications,<sup>99</sup> but the ability to regulate Internet content is not one of them. In addition, under the Trump Administration, the FCC has largely forsworn potential sources of authority that could be marshaled here. Thus, at present, it is unlikely that the FCC will be able to issue the Executive Order's proposed rules.

### A. Proposed Rules Under the Executive Order and NTIA Petition

Executive Order 13,925, initially drafted in August 2019,<sup>100</sup> asserts that "[o]nline platforms are engaging in selective censorship that is harming our national discourse" by flagging content as inappropriate, making unexplained policy changes, and deleting content and entire accounts without warning, rationale, or recourse.<sup>101</sup> The Order identifies Section 230 as the culprit enabling this "censorship" and argues that the statute should be "clarified" in several respects.<sup>102</sup>

The Order directs the Secretary of Commerce to cause the National Telecommunications Information Administration (NTIA) to file a petition for rulemaking with the FCC within 60 days<sup>103</sup> to "expeditiously propose regulations to clarify" that: (1) Section 230(c)(1) does not apply to the

---

<sup>96</sup> 47 U.S.C. § 230(c)(2)(A).

<sup>97</sup> Goldman, *supra* note 75, at 40.

<sup>98</sup> See, e.g., *Domen v. Vimeo, Inc.*, 433 F. Supp. 3d 592, 599, 603–04 (S.D.N.Y. 2020) (dismissing case under Section 230(c)(2)).

<sup>99</sup> See 47 U.S.C. § 303 (setting forth express powers of the FCC).

<sup>100</sup> Margaret Harding McGill & Daniel Lippman, *White House Drafting Executive Order to Tackle Silicon Valley's Alleged Anti-Conservative Bias*, POLITICO (Aug. 7, 2019, 3:07 PM), <https://www.politico.com/story/2019/08/07/white-house-tech-censorship-1639051> [<https://perma.cc/2DQ9-8CRP>].

<sup>101</sup> Exec. Order No. 13,925, 85 Fed. Reg. 34,079, 34,079 (June 2, 2020).

<sup>102</sup> *Id.* at 34,080.

<sup>103</sup> *Id.* at 34,081.

removal of content; and (2) under Section 230(c)(2), “good faith” requires service providers to “provide adequate notice, reasoned explanation, or a meaningful opportunity to be heard”<sup>104</sup> before they can remove a user’s content. The remainder of the Order advances other initiatives ostensibly aimed at eliminating “Tech Bias,” but none involve the FCC or Section 230.<sup>105</sup>

As required by the Executive Order, NTIA filed a petition for rulemaking with the FCC.<sup>106</sup> The FCC has published the petition for comment,<sup>107</sup> and on October 15, 2020, Chairman Ajit Pai stated that “I intend to move forward with a rulemaking to clarify [Section 230’s] meaning.”<sup>108</sup> While Republicans currently control the FCC 3–2, it is not clear whether they have three votes to commence a rulemaking proceeding—at least at present. Following the Executive Order’s release, Republican Commissioner Michael O’Rielly commented that despite harboring concerns about the actions of “liberal tech leaders,” “I’m extremely dedicated to [the] First Amendment which governs much here.”<sup>109</sup> The Trump Administration interpreted this comment as opposition: In September, it withdrew O’Rielly’s re-nomination to the FCC and instead nominated Nathan Simington—a senior NTIA advisor who is said to have played a significant role in drafting NTIA’s petition—to fill O’Rielly’s seat once it is vacated.<sup>110</sup>

NTIA’s petition significantly expands upon the Executive Order’s mandate by asking the FCC to “interpret” Section 230 in a variety of ways that the Order did not specifically request.<sup>111</sup> Notwithstanding this expansion, this Essay addresses only the proposed rules that are directed towards

---

<sup>104</sup> *Id.* The Order also asks for clarification as to whether an action can be “taken in good faith” if it is “deceptive, pretextual, or inconsistent with a provider’s terms of service.” *Id.*

<sup>105</sup> *Id.* at 34,081–82.

<sup>106</sup> Nat’l Telecomms. & Info. Admin., Petition for Rulemaking, RM-11862 (July 27, 2020) [hereinafter NTIA Pet.].

<sup>107</sup> FCC, Public Notice, Petition for Rulemakings Filed, Report No. 3157 (Aug. 3, 2020), <https://docs.fcc.gov/public/attachments/DOC-365914A1.pdf> [<https://perma.cc/4SAZ-YCWU>].

<sup>108</sup> FCC, Statement of Chairman Pai on Section 230 (Oct. 15, 2020), <https://docs.fcc.gov/public/attachments/DOC-367567A1.pdf> [<https://perma.cc/38DC-GFQ9>].

<sup>109</sup> Makena Kelly, *Trump Nominates Social Media Hawk as Next FCC Commissioner*, VERGE (Sept. 15, 2020, 9:38 PM), <https://www.theverge.com/2020/9/15/21438820/fcc-donald-trump-nominate-nathan-simington-commissioner-social-media-section-230-order> [<https://perma.cc/WHL9-BSJ4>].

<sup>110</sup> *Id.*

<sup>111</sup> Most notably, NTIA’s proposed rules state that “[a]n interactive computer service is not being ‘treated as the publisher or speaker of any information provided by another information content provider’ when it actually publishes its own or third-party content.” NTIA Pet., *supra* note 106, at 53 (proposed 47 C.F.R. § 130.01(c)). This would likely gut Section 230(c)(1) as to “publish” content is to make it publicly available—which is what all platforms do. *See Force v. Facebook, Inc.*, 934 F.3d 53, 65 (2d Cir. 2019) (discussing meaning of “publisher”).

constraining decisions to remove or restrict access to online content as that was the focal point of the Executive Order.

As contemplated by the Order, NTIA's proposed rules would preclude the application of Section 230(c)(1) to the act of removing or restricting user content, thus shunting those acts into Section 230(c)(2) alone.<sup>112</sup> The proposed regulations next seek to limit Section 230(c)(2) by (1) replacing its subjective good faith element with one of objective reasonableness;<sup>113</sup> (2) removing the "otherwise objectionable" catch-all category (thus limiting the provision's applicability to the enumerated categories of offensive content);<sup>114</sup> and (3) requiring a service provider to give advance notice and reason for removing or restricting access to user content before doing so, and allow the impacted user a reasonable opportunity to respond.<sup>115</sup> On the last point, service providers need not provide advance notice (i.e., they may remove or restrict access to materials immediately) if they have a reasonable belief that the content is related to criminal activity or would risk imminent physical harm.<sup>116</sup>

#### *B. FCC Rulemaking Authority Under the Communications Act*

Created by the New Deal-era Communications Act of 1934,<sup>117</sup> the FCC is charged with regulating interstate and international communications by radio, television, wire, satellite, and cable.<sup>118</sup> The Telecommunications Act of 1996 updated the Communications Act for the Internet era. Where the Internet is concerned, the degree of regulatory authority depends on whether

---

<sup>112</sup> NTIA Pet., *supra* note 106, at 53 (proposed rule 47 C.F.R. § 130.01(a)) ("Section 230(c)(1) has no application to any interactive computer service's decision, agreement, or action to restrict access to or availability of material provided by another information content provider . . . . Any applicable immunity for matters described in the immediately preceding sentence shall be provided solely by 47 U.S.C. § 230(c)(2).").

<sup>113</sup> NTIA Pet., *supra* note 106, at 55 (proposed rule 47 C.F.R. § 130.02(e)(vi)) (providing that good faith requires, *inter alia*, "an *objectively reasonable belief* that the material falls within one of the listed categories set forth in 47 U.S.C. § 230(c)(2)(A)") (emphasis added).

<sup>114</sup> *Id.* (providing that good faith requires, *inter alia*, "an objectively reasonable belief that the material falls within *one of the listed categories* set forth in 47 U.S.C. § 230(c)(2)(A)") (emphasis added). The proposed rules would also narrowly construe the listed categories. *See id.* at 54–55 (proposed rule 47 C.F.R. § 130.02(a)).

<sup>115</sup> *Id.* at 55 (proposed rule 47 C.F.R. § 130.02(e)(viii)) (requiring "timely notice describing with particularity the interactive computer service's reasonable factual basis for the restriction of access and a meaningful opportunity to respond" subject to exceptions).

<sup>116</sup> *Id.* (providing exceptions where "the interactive computer service has an objectively reasonable belief that the content is related to criminal activity or [where] notice would risk imminent physical harm to others").

<sup>117</sup> Pub. L. No. 73-416, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C.).

<sup>118</sup> *See id.*; *see also About the FCC*, FCC, <https://www.fcc.gov/about/overview> [<https://perma.cc/M8Y8-N4D6>] (agency mission statement).

a service is considered a “telecommunications service” (for which there is comprehensive authority) or an “information service” (for which there is relatively little authority),<sup>119</sup> a distinction added by the 1996 Act. A “‘telecommunications service’ means the offering of telecommunications for a fee directly to the public . . . regardless of the facilities used.”<sup>120</sup> “[T]elecommunications’ means the transmission, between or among points specified by the user, of information of the user’s choosing, without change in the form or content of the information as sent and received.”<sup>121</sup> Basic landline telephone service is the archetype of a telecommunications service.<sup>122</sup> When a system is properly categorized as a “telecommunications service,” its operator—“a telecommunications carrier”—is subject to a panoply of common carrier regulations<sup>123</sup> under Title II of the Communications Act. A common carrier is an entity that has acquired a quasi-public character, from which arises the obligation to carry goods or services for all people indiscriminately and on reasonable terms.<sup>124</sup> Common carrier regulations under Title II of Communications Act include interconnection requirements,<sup>125</sup> price regulation,<sup>126</sup> and anti-discrimination rules.<sup>127</sup>

In contrast, the FCC has no comparable mandate over “information services,” which are services that are capable of “generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing.”<sup>128</sup> Under the Communications Act, these services are “largely unregulated by default.”<sup>129</sup> Further, the Act limits the FCC’s ability to regulate any entity as a common carrier except “to the extent that it is engaged in providing

---

<sup>119</sup> See *U.S. Telecom Ass’n v. FCC*, 825 F.3d 674, 691 (D.C. Cir. 2016) (describing history and development of the distinction between a “telecommunications service” and an “information service”).

<sup>120</sup> 47 U.S.C. § 153(53).

<sup>121</sup> *Id.* § 153(50).

<sup>122</sup> See *U.S. Telecom Ass’n*, 825 F.3d at 691 (observing that the FCC has “subjected basic [telephone] services . . . to common carrier treatment under Title II of the Communications Act”).

<sup>123</sup> *Verizon v. FCC*, 740 F.3d 623, 651–52 (D.C. Cir. 2014) (discussing common carriage generally).

<sup>124</sup> *Id.* at 651 (quoting *Nat’l Assoc. of Regul. Util. Comm’rs v. FCC*, 533 F.2d 601, 608 (1976)) (“[T]he primary *sine qua non* of common carrier status is a quasi-public character, which arises out of the undertaking to carry for all people indifferently.”).

<sup>125</sup> 47 U.S.C. § 201(a).

<sup>126</sup> *Id.* §§ 201(b), 202(a), 205.

<sup>127</sup> *Id.* § 201(b).

<sup>128</sup> *Id.* § 153(24).

<sup>129</sup> *Restoring Internet Freedom*, 33 FCC Rcd. 311, 473–74 ¶ 273 (2018) [hereinafter 2018 FCC Order].



telecommunications services.”<sup>130</sup> Thus, the FCC cannot set rates or prohibit discrimination with respect to information services.<sup>131</sup>

Notably, websites, apps, and other online services have not yet been classified as either a telecommunications service or an information service. It is unlikely, though, that the FCC could classify Facebook or Twitter or the average blog as anything other than an information service.

For one thing, an “information service” expressly includes “electronic publishing,”<sup>132</sup> which describes the activity of every website. Even without the “electronic publishing” example, it is a heavy lift to show that a website could qualify as a telecommunications service. Websites do not just transmit data from one point to another without any change whatsoever: they receive and store user information, reformat that information, and present it in a web interface that allows other users to interact with it. Further, telecommunications services must be provided for “a fee directly to the public” or to users,<sup>133</sup> which would make its application to advertising-based revenue models difficult.

Finally, the FCC will be constrained by its own classification of Internet service providers (ISPs)—entities that connect users to the Internet such as Comcast or AT&T—as information services. In repealing the Obama era FCC’s “net neutrality” rules, the current FCC concluded that while ISPs are primarily carriers of data, they can be considered information services because they perform the ancillary services of domain name lookups<sup>134</sup> and caching (temporarily storing files for quicker access).<sup>135</sup> *A fortiori*, companies whose primary services involve the storage and manipulation of information must also be classified as information services. Accordingly,

---

<sup>130</sup> 47 U.S.C. § 153(51).

<sup>131</sup> *Verizon v. FCC*, 740 F.3d 623, 650–55, 659 (D.C. Cir. 2014) (striking down net neutrality rules as unlawful common carrier regulations). The Court in *Verizon* stated it was “obvious that the Commission would violate the Communications Act were it to regulate broadband providers as common carriers” because of the “Commission’s still-binding decision to classify broadband providers not as providers of ‘telecommunications services’ but instead as providers of ‘information services,’ such treatment would run afoul of section 153(51).” *Id.* at 650 (citation omitted).

<sup>132</sup> 47 U.S.C. § 153(24).

<sup>133</sup> *Id.* § 153(53).

<sup>134</sup> Domain Name Service (DNS) matches web page addresses that users type into their browsers with the Internet Protocol (IP) address of the servers hosting those pages. *See Nat’l Cable & Telecom. Ass’n v. Brand X Internet Servs.*, 545 U.S. 967, 987 (2005). For example, DNS translates “Amazon.com” into “108.174.10.10,” thus making it easier for users to locate the web pages they wish to visit. In *Brand X*, the dissent likened DNS to “scarcely more than routing information, which is expressly excluded from the definition of ‘information service.’” *Id.* at 1012–13 (Scalia, J., dissenting) (quoting 47 U.S.C. § 153(20)). In reply, the majority observed that routing information was not excluded from the definition of “information service.” *Id.* at 999 n.3.

<sup>135</sup> 2018 FCC Order, *supra* note 129, at 325 ¶ 33; *Mozilla Corp. v. FCC*, 940 F.3d 1, 32–35 (D.C. Cir. 2019) (finding FCC’s reliance on caching and DNS to justify reclassification reasonable).

under the overall structure of the Communications Act, the FCC lacks the authority to regulate websites and online applications, which are information services.<sup>136</sup>

*C. NTIA's Attempt to Find Rulemaking Authority Under the Common Carrier Provisions of the Communications Act*

In its petition, NTIA attempts to ground rulemaking authority in the FCC's general authority to make common carrier provisions under Section 201(b) of the Communications Act.<sup>137</sup> This presents a novel use of that provision as it is ostensibly limited to making common carrier regulations,<sup>138</sup> which, as discussed above, may only regulate telecommunications services—and not information services like websites. Section 201(a) of the Communications Act begins with the words, “[i]t shall be the duty of every *common carrier* engaged in interstate or foreign communication by wire or radio,”<sup>139</sup> and Section 201(b) explains that “[a]ll charges, practices, classifications, and regulations for and in connection with *such communication service*, shall be just and reasonable.”<sup>140</sup> After describing additional common carrier-specific issues, Section 201(b) concludes with the following sentence: “The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter.”<sup>141</sup> It is this sentence that NTIA relies upon to issue its proposed Section 230 rules.

NTIA argues that Section 201(b) can and should be invoked to make rules under Section 230 because Section 230 was codified into Chapter 5 of Title 47 and thus falls within “this chapter” of the Act.<sup>142</sup> That Section 230 falls within the same chapter as Section 201(b) is certainly true, but it is less clear that the FCC can make regulations under Section 201(b) that have nothing to do with common carriers. The Supreme Court cases that NTIA cites<sup>143</sup> held that Section 201(b) allows rulemaking under later-enacted provisions (specifically, those added by the 1996 Telecommunications Act),

---

<sup>136</sup> 2018 FCC Order, *supra* note 129, at 473–74 ¶ 273.

<sup>137</sup> 47 U.S.C. § 201(b) (“The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter.”); NTIA Pet., *supra* note 106, at 15–16.

<sup>138</sup> 47 U.S.C. § 201.

<sup>139</sup> *Id.* § 201(a) (emphasis added).

<sup>140</sup> *Id.* § 201(b) (emphasis added).

<sup>141</sup> *Id.*

<sup>142</sup> Chapter 5 of Title 47, titled “Wire or Radio Communication,” encompasses Sections 151 through 621 of Title 47. Section 230 is found in Subchapter II, titled “Common Carriers,” which includes Section 201 through 276.

<sup>143</sup> NTIA Pet., *supra* note 106, at 16–17, 16 n.46.

but the regulations in those cases at least concerned common carriers.<sup>144</sup> Given that Section 201(b) appears to be focused on common carrier regulations, its rulemaking authority grant seems a poor vehicle to use for regulating entities that are not common carriers. And, as discussed further below, there is no mandate for the FCC to “carry out” Section 230.

*D. The FCC’s Lack of Rulemaking Authority Under Section 230*

Notwithstanding the arguments above, Section 230 of the CDA is an unlikely candidate for regulation by the FCC. Section 230 does not once mention the FCC: It does not give the agency express authority to make rules, nor does it create a scheme for the FCC to administer. Instead, the statute’s immunities provide a defense to litigation.

In addition, Section 230(b)’s statements of policy are at odds with regulation of content-related practices. Section 230(b)(2) speaks of Congress’s desire to maintain the free and open market for Internet services “unfettered by Federal or State regulation.”<sup>145</sup> As Representative Christopher Cox, one of Section 230’s co-sponsors put it, this statement of policy establishes that “we do not wish to have content regulation by the Federal Government of what is on the Internet [and] that we do not wish to have a Federal Computer Commission with an army of bureaucrats regulating the Internet.”<sup>146</sup> Co-sponsor and then-Representative Ron Wyden observed that Congress had rejected alternative proposals involving FCC oversight, which he critiqued as requiring “the Federal Government spending vast sums of money trying to define elusive terms that are going to lead to a flood of legal challenges.”<sup>147</sup> In response to NTIA’s petition, Senator Wyden and former Representative Cox confirmed that “[w]e and our colleagues in Congress on both sides of the aisle were emphatic that we were not creating new regulatory authority for the FCC or any other independent agency or executive branch department when we enacted Section 230.”<sup>148</sup>

---

<sup>144</sup> *AT&T Corp. v. Iowa Utils. Bd.*, 525 U.S. 366, 378 n.5 (1999) (involving local competition provisions affecting incumbent local exchange carriers under 47 U.S.C. §§ 251 and 252); *City of Arlington v. FCC*, 569 U.S. 290, 294 (2013) (involving state regulation of siting applications for personal wireless services, a type of common carrier, under 47 U.S.C. § 332).

<sup>145</sup> 47 U.S.C. § 230(b)(2).

<sup>146</sup> 141 CONG. REC. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

<sup>147</sup> *Id.* (statement of Rep. Wyden).

<sup>148</sup> Co-Authors of Section 230 of the Communications Act of 1934, Reply Comments to Petition for Rulemaking to Clarify Provision of Section 230, RM-11862, at 4 (Sept. 17, 2020), <https://ecfsapi.fcc.gov/file/10917190303687/2020-09-17%20Cox-Wyden%20FCC%20Reply%20Comments%20Final%20as%20Filed.pdf> [<https://perma.cc/ZW6C-S5TB>].

Consistent with these views, the FCC has found that Section 230(b) sets forth a “deregulatory policy”<sup>149</sup> and cited it when determining not to classify ISPs as telecommunications carriers and impose common carrier regulations upon them.<sup>150</sup> It would be ironic if the FCC then held that it somehow retained the right to impose content removal regulations on websites, users, and ISPs under Section 230(c).

Finally, any interpretation of Section 230 by the FCC would be an exercise in futility because the FCC cannot actually enforce Section 230’s immunities. Because Section 230 is a litigation defense, its arbiters are the courts. While courts typically defer to agencies in the interpretation of their governing statutes,<sup>151</sup> they may not be so willing to do so here where the FCC does not administer Section 230 and has no agency expertise or experience adjudicating Section 230 cases.<sup>152</sup> In addition, as explained in Part III, the proposed rules are fundamentally inconsistent with Section 230.

### III. THE PROPOSED RULES ARE INCONSISTENT WITH SECTION 230

Rulemaking authority is vested in agencies to fill in the gaps left by Congress in a statute.<sup>153</sup> Rulemaking cannot, however, be used to alter an unambiguous statute.<sup>154</sup> Even where ambiguity exists, an agency cannot promulgate rules that unreasonably interpret the ambiguity<sup>155</sup> or contravene the text of the statute.<sup>156</sup> Here, even assuming the FCC had proper authority, the proposed changes would amend Section 230 without Congress’s consent.

#### A. *The Proposed Limitation of Section 230(c)(1)*

The Executive Order would have the FCC “clarify” that Section 230(c)(2)’s “good faith” requirement exclusively covers content removal decisions. The problem, as the White House sees it, is that if Section 230(c)(1) also applies to content removals, then a service provider can

---

<sup>149</sup> 2018 FCC Order, *supra* note 129, at 349–50 ¶ 61.

<sup>150</sup> *Id.*

<sup>151</sup> See *Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 843 (1984) (explaining that where a “statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency’s answer is based on a permissible construction of the statute”); *City of Arlington v. FCC*, 569 U.S. 290, 301–02 (2013) (holding that *Chevron* applies to both jurisdictional and non-jurisdictional matters).

<sup>152</sup> See *King v. Burwell*, 135 S. Ct. 2480, 2489 (2015) (explaining that no deference is owed to IRS, “which has no expertise in crafting health insurance policy”); *Gonzales v. Oregon*, 546 U.S. 243, 258–69 (2006) (finding no deference owed to DOJ where it lacked authority to issue interpretation).

<sup>153</sup> See *Nat’l Cable & Telecom. Ass’n v. Brand X Internet Servs.*, 545 U.S. 967, 980 (2005).

<sup>154</sup> See *id.* at 986.

<sup>155</sup> *United States v. Home Concrete & Supply, LLC*, 566 U.S. 478, 493 n.1 (2012) (“It does not matter whether the word ‘yellow’ is ambiguous when the agency has interpreted it to mean ‘purple.’”).

<sup>156</sup> *Verizon v. FCC*, 740 F.3d 623, 634–35, 665–66 (D.C. Cir. 2014).

remove content for any reason—whether or not taken in “good faith.”<sup>157</sup> If true, then a service provider’s ability to remove content is not constrained. The Executive Order argues that this renders Section 230(c)(2) useless, and that the canon against surplusage interpretations counsels an interpretation that gives both provisions meaning.<sup>158</sup> Accordingly, the Order argues that Section 230(c)(1) should be limited to immunizing the act of making content public, but not the act of removing or restricting access to content.<sup>159</sup>

The trouble with this surplusage argument is that it is not true. Interpreting Section 230(c)(1) to apply to the decision to remove content does not negate Section 230(c)(2). Instead, the latter “still has work to do.”<sup>160</sup> First, Section 230(c)(1) applies only to publishing decisions made regarding “information provided by another information content provider”—in other words, third-party content.<sup>161</sup> By its terms, this provision would not immunize a website provider’s removal or restriction of its own content. In contrast, Section 230(c)(2) would cover removal of the provider’s own content as well as third party content, as it applies to any “materials” regardless of the author.<sup>162</sup> This immunity could come into play if a website had decided to restrict portions of its content to some users, but not others based upon, for example, the age of the users in question.<sup>163</sup>

Second, because Section 230(c)(1) requires that the defendant be treated as the “publisher,” it does not apply where the service provider has stepped outside of the traditional publisher role.<sup>164</sup> For example, in *Barnes v. Yahoo!, Inc.*, the Ninth Circuit held that a promise to remove content could support a promissory estoppel claim that was not barred by Section 230(c)(1) because it did not implicate the website’s duties as a publisher.<sup>165</sup> Thus, where a website makes an express promise regarding user content that is collateral to its publisher role, Section 230(c)(1) might not apply; however,

---

<sup>157</sup> See *supra* notes 5–10 and accompanying text.

<sup>158</sup> Exec. Order No. 13,925, 85 Fed. Reg. 34,079, 34,081 (June 2, 2020).

<sup>159</sup> *Id.*; see also *e-Ventures Worldwide, LLC v. Google, Inc.*, No. 2:14-cv-646, 2017 WL 2210029, at \*3 (M.D. Fla. Feb. 8, 2017).

<sup>160</sup> *Nielsen v. Preap*, 139 S. Ct. 954, 969, 971 (2019) (in different statutory context, declining to apply canon regarding surplusage interpretations).

<sup>161</sup> 47 U.S.C. § 230(c)(1).

<sup>162</sup> See *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1102 (9th Cir. 2009).

<sup>163</sup> See *Ashcroft v. ACLU*, 535 U.S. 563, 582 n.14 (2002) (recognizing existence of “adult identification screens” to verify age of users); *PSINet, Inc. v. Chapman*, 362 F.3d 227, 252 (4th Cir. 2004) (Niemeyer, J., dissenting) (explaining that “technological mechanisms exist to create adult zones by using credit cards, passwords, PIN identification, adult verification services, and website self-identification methods”).

<sup>164</sup> 47 U.S.C. § 230(c)(1).

<sup>165</sup> *Barnes*, 570 F.3d at 1102, 1109.

Section 230(c)(2) could still apply if the underlying action is to remove content.

Third, Section 230(c)(2) actually contains two subparts. The second subpart, paragraph (B), is not impacted by construing Section 230(c)(1) to include or exclude content removal. Section 230(c)(2)(B) allows entities to create and distribute tools that allow users and service providers to restrict access to content as permitted by paragraph (A).<sup>166</sup> Thus, Facebook or Twitter may, without liability, enable users to block other people, and other companies may create software that allows people to filter the content that they view.<sup>167</sup> The right in Section 230(c)(2)(B) incorporates by reference the definitional elements of Section 230(c)(2)(A) and has no parallel in Section 230(c)(1).<sup>168</sup>

Considering all of the ways that Section 230(c)(2) may apply where Section 230(c)(1) may not, the judicial preference of avoiding surplusage interpretations does not apply.<sup>169</sup>

### B. *The Proposed Restriction of Section 230(c)(2)*

NTIA’s petition restricts Section 230(c)(2) to the expressly enumerated categories of content and then defines those categories narrowly.<sup>170</sup> In doing so, the petition reads the term “otherwise objectionable” out of the statute.<sup>171</sup> NTIA relies on the statutory interpretation canon *esjudem generis*<sup>172</sup> to interpret that term but ends up actually eliminating it entirely.<sup>173</sup> This is not a reasonable construction since it fails to give meaning to the words “otherwise objectionable,” thus committing the sin of surplusage interpretations that the petition rails about elsewhere.<sup>174</sup> In addition, as discussed above, the force of *esjudem generis* is blunted where the enumerated terms speak to vastly different matters, as is the case in the types of material described in Section 230(c)(2)(A).<sup>175</sup>

<sup>166</sup> 47 U.S.C. § 230(c)(2)(B).

<sup>167</sup> See *Fehrenbach v. Zeldin*, No. 17-CV-5282, 2018 WL 4242452, at \*5 (E.D.N.Y. Aug. 6, 2018) (dismissing claim that Facebook facilitated content removal by others).

<sup>168</sup> Compare 47 U.S.C. § 230(c)(1), with *id.* § 230(c)(2)(B).

<sup>169</sup> See *Nielsen v. Preap*, 139 S. Ct. 954, 969 (2019) (rejecting application of canon against surplusage where statute “still has work to do”).

<sup>170</sup> NTIA Pet., *supra* note 106, at 54–55 (proposed rules 47 C.F.R. §§ 130.02, 130.03).

<sup>171</sup> 47 U.S.C. § 230(c)(2)(A).

<sup>172</sup> NTIA Pet., *supra* note 106, at 31–32.

<sup>173</sup> *Id.* at 54 (proposed rule 47 U.S.C. § 130.02(e)(vi)) (requiring “objectively reasonable belief that the material falls within one of the listed categories set forth in 47 U.S.C. § 230(c)(2)(A)”).

<sup>174</sup> See *id.* at 28–29.

<sup>175</sup> 47 U.S.C. § 230(c)(2)(A) (enumerating “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable” material).

### C. *The Proposed Introduction of an Objective Standard*

As written, Section 230(c)(2) protects a service provider that acts in “good faith” to remove content that it “considers to be . . . objectionable.”<sup>176</sup> This speaks to a purely subjective good faith standard.<sup>177</sup> Despite this, NTIA proposes to change the mental state to one of reasonableness. But because terms like “good faith” and “reasonableness” have well-settled meanings under the common law, it is presumed that, unless Congress specifically provides otherwise, statutes should be interpreted with those standards in mind.<sup>178</sup> Since Congress did not provide a non-standard definition of “good faith” (or any definition for that matter), it must be assumed that the term retains its ordinary common law meaning.

To that end, “courts interpreting other federal statutes have traditionally interpreted ‘good faith’ to encompass a subjective standard.”<sup>179</sup> As such, “the objective reasonableness standard is distinct from the subjective good faith standard, and . . . Congress understands this distinction.”<sup>180</sup> Because the two standards are mutually exclusive,<sup>181</sup> swapping one for the other would be akin to rewriting the statute.

### D. *The Proposed Due Process Requirements*

The Executive Order proposes that immunity should not apply to those service providers who, in removing content, “fail[] to provide adequate notice, reasoned explanation, or a meaningful opportunity to be heard.”<sup>182</sup> NTIA’s petition recasts this burden by requiring service providers to (1) furnish “timely notice” (2) “describ[e] with particularity the interactive computer service’s reasonable factual basis for the restriction of access,” and (3) provide users with “a meaningful opportunity to respond.”<sup>183</sup> Advance notice is not required, however, if “the interactive computer service has an objectively reasonable belief that the content is related to criminal activity or

---

<sup>176</sup> *Id.*

<sup>177</sup> See *Domen v. Vimeo, Inc.*, 433 F. Supp. 3d 592, 603 (S.D.N.Y. 2020) (focusing on Vimeo’s “subjective” good faith).

<sup>178</sup> *Neder v. United States*, 527 U.S. 1, 21 (1999) (“It is a well-established rule of construction that where Congress uses terms that have accumulated settled meaning under the common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of these terms.”) (quotation marks and citation omitted).

<sup>179</sup> *Rossi v. Motion Picture Ass’n of Am., Inc.*, 391 F.3d 1000, 1004 (9th Cir. 2004) (holding that 17 U.S.C. § 512(c)’s reference to “good faith belief” referred to subjective good faith).

<sup>180</sup> *Id.*

<sup>181</sup> See *Manuel v. City of Joliet*, 137 S. Ct. 911, 925 (2017) (Alito, J., dissenting) (“These two standards—one subjective and the other objective—cannot co-exist.”).

<sup>182</sup> Exec. Order No. 13,925, 85 Fed. Reg. 34,079, 34,081 (June 2, 2020).

<sup>183</sup> NTIA Pet., *supra* note 106, at 55 (proposed rule 47 C.F.R. 130.02(e)(viii)).

such notice would risk imminent physical harm to others.”<sup>184</sup> It is difficult to see how these procedural rules can be fashioned from thread as bare as “good faith,” especially given Congress’s policy goals in enacting Section 230.<sup>185</sup> As explained above, “good faith” is a subjective mental element. And, as Professor David Pozen observes, “[c]lassic formulations of legal bad faith look to the actor’s state of mind and, above all, to her honesty and sincerity.”<sup>186</sup> It does not, however, require procedural due process.<sup>187</sup>

Moreover, the statute is quite clear in what it requires of service providers—and that is very little. The only affirmative obligation in the entire statute is Section 230(d)’s unenforceable requirement that service providers inform users that filtering technologies are available.<sup>188</sup> The existence of this singular obligation indicates that Congress knew how to impose affirmative obligations on service providers, but declined to do so when it came to content moderation.<sup>189</sup> Consistent with this view, the immunity applies “even when self-regulation is unsuccessful, or completely unattempted.”<sup>190</sup>

In addition to these statutory interpretation hurdles, the notice requirements create another concern that bears mentioning in brief. Specifically, they raise the specter of compelled speech in violation of the First Amendment. By requiring service providers to provide notice and to articulate reasons for a proposed removal of content—as well the requirement that they continue hosting objectionable content for a period after notice has been delivered—the rules may very well abridge the First Amendment right not to speak.<sup>191</sup>

---

<sup>184</sup> *Id.*

<sup>185</sup> See discussion *infra* Section IV.

<sup>186</sup> David E. Pozen, *Constitutional Bad Faith*, 129 HARV. L. REV. 885, 892 (2016).

<sup>187</sup> For example, many judicial and governmental bodies make decisions every day without providing reasons. See Frederick Schauer, *Giving Reasons*, 47 STAN. L. REV. 633, 634 (1995) (providing examples including the Supreme Court denying certiorari, appellate judges ruling from the bench, and trial judges overruling objections).

<sup>188</sup> 47 U.S.C. § 230(d). Congress did not provide in the statute a remedy for violation thereof. *Id.*

<sup>189</sup> Here, the maxim *expressio unius est exclusio alterius* (to say one thing is to exclude another) comes into play. See *Tenn. Valley Auth. v. Hill*, 437 U.S. 153, 188 (1978) (holding that Congress’s decision to include hardship exemptions in a statute indicated the lack of additional non-hardship-based exemptions).

<sup>190</sup> See *Barrett v. Rosenthal*, 146 P.3d 510, 523 (Cal. 2006) (discussing lack of obligations under Section 230(c)(1)); *Green v. Am. Online (AOL)*, 318 F.3d 465, 472 (3d Cir. 2003) (explaining that “Section 230(c)(2) does not *require* AOL to restrict speech; rather it allows AOL to establish standards of decency without risking liability for doing so”).

<sup>191</sup> A full discussion of this issue is beyond the scope of this Essay. For a general discussion of the First Amendment right against compelled speech, see Caroline Mala Corbin, *The First Amendment Right Against Compelled Listening*, 89 B.U. L. REV. 939, 977–80 (2009). Certain commenters in the FCC



## IV. POLICY CONSIDERATIONS

While some believe that voluntary measures by large social media platforms to enhance content moderation transparency and provide recourse mechanisms are welcome,<sup>192</sup> the Section 230 immunities should not be conditioned upon providing such measures. Congress explicitly endorsed this policy choice in enacting Section 230.<sup>193</sup> Indeed, one court concluded that requiring a service provider to discuss its reasons for removing content would be inconsistent with these goals.<sup>194</sup> Congress usually does not “hide elephants in mouseholes,”<sup>195</sup> and so it would be surprising if Congress sought to undermine its own goals through an idiosyncratic conception of “good faith.”

Moreover, moderating content is a complex endeavor, particularly for companies that are operating at scale, and prescriptive content moderation rules would likely cause unintended harms, such as increasing moderation challenges, enabling more harmful speech online, and rendering the immunity provided by Section 230(c)(2) essentially nonexistent.

A. *Increased Moderation Challenges*

Requiring advance notice or individualized reasons for content removal will make moderation efforts less effective and more costly. First, these duties cannot fully be performed by automated technologies, which major platforms use, in conjunction with human review, to address the sheer volume of content posted by users.<sup>196</sup> Automated techniques include using

---

proceeding have raised the point about compelled speech. *See, e.g.*, TechFreedom, Comments on Petition for Rulemaking to Clarify Provisions of Section 230, RM-11862, at 71–73 (Sept. 2, 2020), <https://ecfsapi.fcc.gov/file/10903920204512/NTIA%20230%20Petition%20Comments%20-%209.2.2020.pdf> [<https://perma.cc/Y72Z-HVCQ>]; Professors Christopher Terry and Daniel Lyons, Reply Comments on Petition for Rulemaking to Clarify Provisions of Section 230, RM-11862, at 3–4 (Sept. 10, 2020), <https://ecfsapi.fcc.gov/file/109101724016162/2020%20Terry%20and%20Lyons%20Sec%20230%20Comments.pdf> [<https://perma.cc/LX3F-KUCM>].

<sup>192</sup> For example, the Santa Clara Principles on user content set forth voluntary principles for content moderation transparency and recourse. *See* THE SANTA CLARA PRINCIPLES ON TRANSPARENCY AND ACCOUNTABILITY IN CONTENT MODERATION, <https://santaclaraprinciples.org/> [<https://perma.cc/6K3Y-QMEQ>].

<sup>193</sup> *See supra* notes 29–32 and accompanying text.

<sup>194</sup> *See* *Holomaxx Tech. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1105 (N.D. Cal. 2011) (finding that imposing “a duty [on Microsoft] to discuss in detail its reasons for blocking Holomaxx’s communications or to provide a remedy for such blocking . . . would be inconsistent with the intent of Congress”).

<sup>195</sup> *Whitman v. Am. Trucking Ass’ns*, 531 U.S. 457, 468 (2001).

<sup>196</sup> *Force v. Facebook, Inc.*, 934 F.3d 53, 60 (2d Cir. 2019) (describing Facebook’s efforts to combat extremist content on its platform through the combination of internal procedures, user reports, and experimental artificial intelligence).

keywords to block or identify content,<sup>197</sup> filtering suspect IP addresses,<sup>198</sup> detecting suspicious activity traffic patterns,<sup>199</sup> fingerprinting media files and comparing them to reference databases, and hash-blocking files.<sup>200</sup> These tools are particularly useful when combatting problems of scale like spam and inauthentic content, which can be automated by bad actors. If these tools cannot be used, spam and inauthentic content will proliferate.

Platforms could try to compensate by increasing the size of their human review teams, but this comes with additional costs and challenges. As Professor Tim Wu has observed, software-based solutions enjoy an “undeniable comparative advantage” over human employees when it comes to “scale, speed, and efficacy.”<sup>201</sup> Human review is particularly ill-suited to problems caused by automated software like scripts or bots—the tools of choice for spammers, hackers, and other bad actors.<sup>202</sup> While human review is an acceptable (and perhaps even the preferred<sup>203</sup>) method for reviewing

---

<sup>197</sup> See *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 528 (S.D.N.Y. 2013) (describing keyword-based tools), *aff'd in part, rev'd in part*, 826 F.3d 78 (2d Cir. 2016).

<sup>198</sup> See *Optinrealbig.com, LLC v. Ironport Sys., Inc.*, 323 F. Supp. 2d 1037, 1040–41 (N.D. Cal. 2004) (describing use of IP addresses to combat spam).

<sup>199</sup> See Kurt Wagner, *Facebook Found a New Way to Identify Spam and False News Articles in Your News Feed* (June 30, 2017, 2:00 PM), <https://www.vox.com/2017/6/30/15896544/facebook-fake-news-feed-algorithm-update-spam> [<https://perma.cc/5FN5-QW6L>] (explaining that Facebook algorithms determine fake news in part by examining links shared by persons posting content more than fifty times per day).

<sup>200</sup> Klonick, *supra* note 11, at 1636–37 (describing “ex ante,” i.e., pre-publication, automated moderation methods).

<sup>201</sup> Tim Wu, *Will Artificial Intelligence Eat the Law? The Rise of Hybrid Social-Ordering Systems*, 119 COLUM. L. REV. 2001, 2021 (2019) (“Code is fast, can scale to meet the size of the problem, and operates at low marginal cost.”).

<sup>202</sup> *What is a Spam Bot? How Spam Comments and Spam Messages Spread*, CLOUDFLARE, <https://www.cloudflare.com/learning/bots/what-is-a-spambot/#:~:text=%7C%20How%20Spam%20Comments%20and%20Spam.operate%20stolen%20social%20media%20accounts> [<https://perma.cc/6DB2-53W3>]; see also Recent Development, *Splog! Or How to Stop the Rise of a New Menace on the Internet*, 19 HARV. J.L. & TECH. 467, 469–70, 476 (2006) (describing the proliferation of link and comment spam caused by automated software and calling for regulation of the use of scripts, bots, and other programs to quickly post multiple messages on these sites).

<sup>203</sup> Automated technologies may be more efficient, but they may miss nuances and may lead to either (or both) an over-removal of lawful content (false positives) or an under-removal of illicit content (false negatives). See Michal Lavi, *Do Platforms Kill?*, 43 HARV. J.L. & PUB. POL'Y 477, 499–500 (2020) (“[T]hus far, technological suggestions for moderation of terrorist content have been rejected. There is concern that algorithms will fail to capture context accurately, resulting in both over-removal of content that is not incitement . . . and under-removal of inciting content that would allow harmful content to spread.”). In addition, “data-driven, algorithmic processes multiply both obstacles to accountability and opportunities for cooptation of accountability structures.” Julie E. Cohen, *Internet Utopianism and the Practical Inevitability of the Law*, 18 DUKE L. & TECH. REV. 85, 95 (2019). As a result of these drawbacks, “[h]uman resources remain vitally important to when and how the major platforms publicly distribute user-generated content.” Olivier Sylvain, *Recovering Tech’s Humanity*, 119 COLUM. L. REV. F. 252, 260 (2019).

certain types of content on an individualized basis, it is not well suited to situations where a bad actor is flooding a site with thousands of posts in a very short time period. This scenario presents a problem of scale that is best addressed by technical solutions to, among other things, detect and block suspicious traffic patterns.<sup>204</sup> In addition, not every platform has the resources to hire a team of thousands.

At the same time, human review productivity will likely decrease as reviewers would be forced to provide detailed reasons when removing content. At present, most sites provide only the nature of the violation (e.g., “pornography”). Such a response would, presumably, not suffice under the proposed rules, where the service provider must issue a written notice “describing with particularity” the “factual basis” for its decision.<sup>205</sup> Taking the time to, for example, watch the entirety of a video, and then detail the reasons for removal (e.g., “At time index 2:30, the individuals in the video participate in a sexual act, to wit . . .”) will almost certainly slow down content removals and limit the number of removals that each human reviewer can accomplish within a workday.<sup>206</sup>

Furthermore, platforms that rely on volunteer moderators to achieve scale will suffer. Section 230 currently protects every volunteer moderator of a forum when they remove content. At present, individual employees who make decisions about user content are covered by Section 230 since they themselves are “users” of interactive computer services.<sup>207</sup> If the Order’s suggested rules apply, however, unpaid volunteers who serve as moderators of interest-based forums<sup>208</sup> could be exposed to personal liability. This makes

---

<sup>204</sup> Jonathan I. Ezor, *Busting Blocks: Revisiting 47 U.S.C. § 230 to Address the Lack of Effective Legal Recourse for Wrongful Inclusion in Spam Filters*, 17 RICH. J.L. & TECH. 1, 14–18 (2011) (describing technologies including block lists and filters for addressing email spam).

<sup>205</sup> NTIA Pet., *supra* note 106, at 55 (proposed rule 47 C.F.R. 130.02(e)(viii)).

<sup>206</sup> There is also a cost exacted on the human reviewers. In May 2020, Facebook agreed to provide a settlement fund of \$52 million to former content moderators who suffered post-traumatic stress disorder as a result of their work reviewing graphic and objectionable content in connection with a putative class action lawsuit. See *SCOLA V. FACEBOOK PROPOSED SETTLEMENT*, <https://contentmoderator.settlement.com/> [<https://perma.cc/6BU3-W3J4>] (official settlement website for *Scola v. Facebook, Inc.*, No. 18-civ-05135 (Cal. App. Dep’t Super. Ct. 2019)). Final approval of the settlement is pending.

<sup>207</sup> See 47 U.S.C. §§ 230(c)(1), (c)(2)(A); see also, e.g., *Batzel v. Smith*, 333 F.3d 1018, 1030 (9th Cir. 2003) (“[T]he language of § 230(c)(1) confers immunity not just on ‘providers’ of such services, but also on ‘users’ of such services.”).

<sup>208</sup> See J. Nathan Matias, *What Just Happened on Reddit? Understanding the Moderator Blackout*, SOC. MEDIA COLLECTIVE (July 13, 2015), <https://socialmediacollective.org/2015/07/09/what-just-happened-on-reddit-understanding-the-moderator-blackout/> [<https://perma.cc/XS77-BZQT>] (estimating that nearly 100,000 people volunteer as moderators of online communities on Reddit known as “subreddits”).

a difficult and uncompensated job<sup>209</sup> even less attractive. Without a willing pool of moderators, websites will have to choose between devoting more resources to content moderation or deciding to forego content moderation altogether.

Faced with increased costs, some companies will decide that the benefits of hosting user feedback are outweighed by the cost of having to moderate it and will opt to shut it down. This will be particularly true where user content is an ancillary feature of a company's website. For example, local newspapers, already struggling to stay in business, might cut off "below the line" comments sections on their stories.<sup>210</sup> Similarly, online retailers and aggregators may stop allowing user reviews.<sup>211</sup>

Well-funded social media platforms will likely invest in more people, but new entrants do not have this luxury.<sup>212</sup> And given that there is little evidence that consumers want less moderation in their social media platforms, startups will suffer to gain traction.<sup>213</sup> Social media as a sector could therefore become less attractive to investment.<sup>214</sup> This will reduce competition, thus entrenching the very "titans" the Executive Order decries.<sup>215</sup>

### B. More Harmful Speech Online

Under the Executive Order and NTIA's proposed regulations, the immunity for content removal would be limited to the categories of harmful content expressly enumerated in the statute. This means that service providers will only be protected from civil liability when they remove (1)

<sup>209</sup> See Robert Peck, *The Punishing Ecstasy of Being a Reddit Moderator*, WIRED (Mar. 21, 2019, 6:00 AM), <https://www.wired.com/story/the-punishing-ecstasy-of-being-a-reddit-moderator/> [<https://perma.cc/CCA2-3RNQ>] (describing challenges of being a volunteer moderator).

<sup>210</sup> See Clothilde Goujard, *Why News Websites Are Closing Their Comments Sections*, MEDIUM (Sept. 8, 2016), <https://medium.com/global-editors-network/why-news-websites-are-closing-their-comments-sections-ea31139c469d> [<https://perma.cc/Q9EG-4GLJ>].

<sup>211</sup> Even product reviews can contain speech that expresses social and political viewpoints. See Andrew Adam Newman, *Playmobil Finds Fun in the Police State*, N.Y. TIMES (Feb. 15, 2009), <https://www.nytimes.com/2009/02/16/business/media/16playmobil.html> [<https://perma.cc/C77S-E7KG>] (describing reviews on Amazon.com of toy airport security playset in which users commented on the security state and racial profiling).

<sup>212</sup> See Goldman, *supra* note 33, at 8 ("If new entrants had to develop industrial-grade content moderation procedures from day one, we'd see far fewer new entrants.")

<sup>213</sup> See Tim Miller & Hannah Yoest, *The Gross Hellscape that Awaits Ted Cruz on Parler*, BULWARK (June 26, 2020), <https://thebulwark.com/the-gross-hellscape-that-awaits-ted-cruz-on-parler/> [<https://perma.cc/B9LU-VLNA>].

<sup>214</sup> Uncertainty about copyright infringement in the late 1990s caused a "localized investment drought . . . amidst the general dot-com deluge." STEPHEN WITT, *HOW MUSIC GOT FREE: A STORY OF OBSESSION AND INVENTION* 121 (2015).

<sup>215</sup> Exec. Order No. 13,925, 85 Fed. Reg. 34,079, 34,080 (June 2, 2020).

pornography and other adult-related materials, (2) excessively violent content, and (3) harassing speech. This leaves a world of harmful content online: Hate speech, fake news, and even defamation—which animated Section 230—would no longer be covered. Without protections, some companies may choose not to expand categories of prohibited content or to vigorously enforce unprotected categories. This risks a proliferation of harmful content on Internet platforms.

Hate speech presents a particular problem and is a glaring (and perhaps telling) omission from the Executive Order and NTIA’s petition. The very purpose and effect of hate speech is to diminish speech and public participation by targeted groups.<sup>216</sup> As Steve Huffman, Reddit’s CEO and Co-Founder, recently stated, “[t]here’s certain speech—for example, harassment and hate—that prevents other people from speaking.”<sup>217</sup> Notably, one Trump-appointed judge echoed Huffman’s concern in voting to allow President Trump to block users in his Twitter feed because having a forum “overrun with harassment, trolling, and hate speech” will lead to less speech, not more.<sup>218</sup>

Misinformation, another category noticeably left unprotected, would also likely proliferate. As with hate speech, misinformation can cause real world harms. Incorrect medical advice can be fatal, while voting misinformation can undermine democracy. The reply that “more speech” is the best way to counteract these harms is unsatisfactory. Content like fake news propagates far more rapidly and widely than truthful information and is thus impervious to counterspeech.<sup>219</sup>

And even where Section 230(c)(2) would continue to apply, the proposed rules would require service providers to keep certain types of content online until the posting user has a reasonable opportunity to respond, thus further increasing the moderation challenges described above. While the rules provide an exception for cases where the provider reasonably believes that the content violates criminal law, this would not address many common

---

<sup>216</sup> Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435, 1147–50 (2011).

<sup>217</sup> Kevin Roose, *Reddit’s C.E.O. on Why He Banned ‘The\_Donald’ Subreddit*, N.Y. TIMES (June 30, 2020), <https://www.nytimes.com/2020/06/30/us/politics/reddit-bans-steve-huffman.html?action=click&module=Top%20Stories&pgtype=Homepage> [https://perma.cc/JX88-B7XN].

<sup>218</sup> *Knight First Am. Inst. v. Trump*, 953 F.3d 216, 231 (2d Cir. 2019) (Park, J., dissenting from denial of rehearing en banc).

<sup>219</sup> Caroline Mala Corbin, *The Unconstitutionality of Government Propaganda*, OHIO STATE L. REV., (forthcoming 2020) (manuscript at 29–30), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3552222](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3552222) [https://perma.cc/46RQ-VHKW] (explaining that truthful statements are far less likely to be retweeted than lies).

types of harmful content.<sup>220</sup> Take pornography for example. In the United States, content depicting sexual acts—i.e., pornography—is legal. As a result, to earn protection under Section 230(c)(2), service providers would have to give posting users notice and an opportunity to respond before they could remove or even restrict access to pornographic content. In the meantime, the provider will be displaying this content to an audience that may include children.

Perhaps even worse than pornography are forms of harassment. While extreme cases of harassment can be illegal, mere acts of trolling and insults are not. Such toxic content harms the civil discourse by making people less likely to participate in the first place. What is more, “the burdens of dealing with the production of incendiary speech in social media are not borne equally: such speech appears to disproportionately target women and people of color, especially those who use social media platforms to speak up against perceived injustice.”<sup>221</sup> By delaying the removal of harassing content, the Order allows harassers to win.

### C. *An Illusory Immunity*

As a practical matter, even where Section 230(c)(2) applies, if the Executive Order were to have full sway, the degree of immunity provided would be minimal, at best. Whereas the assertion of today’s version requires only a showing of subjective good faith, the President’s version requires that a defendant satisfy a whole panoply of affirmative requirements.<sup>222</sup> The existence of so many requirements makes it unlikely that the affirmative defense could be won on a motion to dismiss. For example, imagine a case where a plaintiff sues, claiming that the defendant has wrongfully removed his videos. He is not obligated to anticipate Section 230 and provide facts relating to the service provider’s actions,<sup>223</sup> so he merely alleges that the service provider has acted wrongfully. In most courts, the defendant likely

---

<sup>220</sup> See discussion *supra* Section III.D.

<sup>221</sup> Lyrissa Barnett Lidsky & Linda Riedemann Norbut, *#I [Hate] U: Considering the Context of Online Threats*, 106 CALIF. L. REV. 1885, 1905–06 (2018); see also, e.g., Tiara Quintana, *What’s in a “Like”?: The Union Interest in Regulating Social Media Use*, 51 U.S.F. L. REV. 147, 152 (2017) (“[T]rolling, hate speech, and online harassment disparately impact women, as a study from 2000–2012 reported that 72.5% of online harassment targeted females.”); Thaddeus Houston, *Constitutional Drag Race: Anonymous Online Speech After Digital Music News v. Superior Court*, 30 BERK. TECH. L. J. 1243, 1247 (2015) (“Pseudonymous trolls also have persistent and troubling misogynistic tendencies.”); *id.* at 1248 (“Another more recent example is ‘Gamergate,’ where female members of the video-gaming community have suffered unjustified real-world consequences for speaking out on the role of women in the video game industry, beginning with waves of attacks by pseudonymous trolls.”).

<sup>222</sup> See discussion *supra* Section III.C.

<sup>223</sup> See *Flying Food Grp., Inc. v. NLRB*, 471 F.3d 178, 183 (D.C. Cir. 2006) (“[A] plaintiff is not required to negate an affirmative defense in his complaint.”) (citation and quotation marks omitted).

will not be able to, in an early motion, introduce facts showing that it provided notice and reasons.<sup>224</sup> The case must then proceed to discovery, which can be costly, and a trial, unless the court grants summary judgment. All of this changes the cost equation for the service provider. No longer does Section 230 provide an immunity at relatively low cost; instead, it provides an immunity that can only be achieved after substantial (and costly) litigation. Faced with the prospect of costly litigation, service providers may well take the path of least resistance: decline to remove content in close cases or cases where the user strenuously objects and threatens a lawsuit. The result is more harmful speech online.

#### CONCLUSION

Contrary to the White House's belief, the FCC cannot modify Section 230 in the guise of interpreting it. The FCC lacks broad authority to regulate the Internet and has closed off possible avenues of regulatory authority in the net neutrality proceedings. In addition, the rules proposed by the Executive Order are inconsistent with Section 230's plain text and purpose. Finally, the Order's proposed rules requiring due process would create uncertainty where none exists now, make hosting user speech more costly, and burden efforts to remove harmful content. This will lead to less beneficial speech, not more.

---

<sup>224</sup> See Fed. R. Civ. P. 12(d) (providing that "if . . . matters outside the pleadings are presented to and not excluded by the court, the motion [to dismiss] must be treated as one for summary judgment" and that "[a]ll parties must be given a reasonable opportunity to present all the material that is pertinent to the motion").