COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

November 29, 2021

To: Subcommittee on Communications and Technology Members and Staff

Fr: Committee on Energy and Commerce Staff

Re: Hearing on "Holding Big Tech Accountable: Targeted Reforms to Tech's Legal Immunity"

On **Wednesday, December 1, 2021, at 10:30 a.m. (EST), in the John D. Dingell Room, 2123 of the Rayburn House Office Building, and via Cisco Webex online video conferencing**, the Subcommittee on Communications and Technology will hold a hearing entitled, "Holding Big Tech Accountable: Targeted Reforms to Tech's Legal Immunity."

I. BACKGROUND

A. Social Media Use

Social media platforms are a major source of entertainment, personal and familial connections, news, and advertising.[1] Research indicates than seven in ten Americans use social media platforms, with Facebook (now rebranded as Meta) and YouTube the most popular overall.[2] The popularity of the top platforms differ by age and demographics.[3] A 2018 Pew Research report on teen social media usage found that 45 percent of teens said they are "online constantly," and that YouTube, Instagram and Snapchat are the most frequently used social media platforms.[4] For young adults, Instagram, Snapchat, and TikTok are most popular.[5]

Among other things, social media platforms allow users to post their own user generated content.[6] While some such platforms allow users to communicate in a decentralized manner that focuses on allowing individual users to decide what they see and in what form they see it, other

---

[1] Pew Research Center, *Social Media Fact Sheet* (April 7, 2021) (www.pewresearch.org/internet/fact-sheet/social-media/).

[2] Pew Research Center, *Social Media Use in 2021* (April 7, 2021) (www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/).

[3] *See* note 1.

[4] Pew Research Center, *Teens, Social Media, and Technology 2018* (May 21, 2018) (www.pewinternet.org/wp-content/uploads/sites/9/2018/05/PI_2018.05.31_TeensTech_FINAL.pdf).

[5] *See* note 2.

[6] *See, e.g., id*.

platforms curate a user's experience on the platform for the users.[7] Of course, many platforms provide a mix of both allowing users to direct some choices while the platform itself makes some choices.[8] For example, a social media platform may opt to allow a user to decide which users it prefers by allowing the users to follow or subscribe to certain other users on the platform, but that platform may decide how to order content from each of those selected users.[9] Such a platform may also recommend content a user has not decided to follow or content to which a user has not subscribed.[10]

B. Reported Harms Associated with Social Media Use

Some argue that social media platforms can harm their users through the decisions the platforms make regarding how to display user generated content including, targeting, ordering, or recommending certain content, among other things.[11] According to a 2021 Anti-Defamation League survey, 41 percent of Americans experienced online harassment over the past year, with 27 percent experiencing severe online harassment, which includes "sexual harassment, stalking, physical threats, swatting, doxing and sustained harassment."[12] Scholars have documented that the use of algorithms by online platforms to target advertisements related to employment, housing, and credit can lead to discrimination and exclusion.[13]

Concerns have been raised specifically about the harms to children perpetrated by social media algorithms.[14] Studies have documented YouTube algorithms that deliver disturbing content to very young children.[15] Internal company documents have demonstrated that Facebook

---

[7] *See Why Tech Platforms Should Give Users More Control — And How They Can Do It,* Medium (Mar. 27, 2018) (dangillmor.medium.com/why-tech-platforms-should-give-users-more-control-and-how-they-can-do-it-6c6c48ab90c0).

[8] *Id.*

[9] *Id.*

[10] TikTok, *How TikTok Recommends videos #ForYou* (June 18, 2020) (newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you).

[11] *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, The Wall Street Journal (Sept. 14, 2021) (www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739).

[12] Anti-Defamation League, *Online Hate and Harassment: The American Experience 2021* (Mar. 2021) (www.adl.org/online-hate-2021).

[13] Pauline T. Kim, *Manipulating Opportunity*, Virginia Law Review (June 1, 2020); Olivier Sylvain, *Discriminatory Designs on User Data*, Knight First Amendment Institute at Columbia University (Apr. 1, 2018).

[14] Bruce Reed and James Steyer, *Why Section 230 Hurts Kids*, Protocol (Dec. 8, 2020). (www.protocol.com/why-section-230-hurts-kids).

[15] Kostantinos Papadamou et al., *Disturbed YouTube for Kids: Characterizing and Detecting Inappropriate Videos Targeting Young Children*, Proceedings of the International AAAI Conference on Web and Social Media (May 26, 2020) (ojs.aaai.org/index.php/ICWSM/article/view/7320).

executives knew that the content on its platform, Instagram was "toxic" for teenage girls, leading them to having eating disorders and suicidal thoughts, but the company did nothing to address it.[16]

For several years, reports have indicated that the algorithms and recommendation tools for many popular social media sites were responsible for the appeal of extremist groups and the prevalence of divisive and racist content.[17] The Federal Bureau of Investigation had warned as well that "[i]nternational and domestic violent extremists have developed an extensive presence on the Internet through messaging platforms and online images, videos, and publications. These facilitate the groups' ability to radicalize and recruit individuals who are receptive to extremist messaging."[18]

And, since the beginning of the coronavirus disease of 2019 (COVID-19) pandemic, platforms have spread substantial amounts of misinformation about COVID-19 regarding the severity of the virus and the safety and efficacy of COVID-19 vaccines.[19] In addition, security experts warned social media companies during and after the November 2016 election that their platforms were being used by foreign governments to disseminate information to manipulate public opinion.[20] This trend continued during and after the November 2020 election, often fomented by domestic actors, with rampant disinformation about voter fraud, defective voting machines, and premature declarations of victory.[21]

Some experts point to the algorithms implemented by platforms that prioritize user engagement and revenue as a major factor in the spread of problematic content. According to Dr. Hany Farid, "[t]hese algorithms have learned that divisive, hateful, and conspiratorial content

---

[16] *Facebook Knows Instagram is Toxic for Teen Girls, Company Documents Show*, Wall Street Journal (Sept. 14, 2021) (www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=hp_lead_pos7&mod=article_inline).

[17] *Facebook Executives Shut Down Efforts To Make The Site Less Divisive*, Wall Street Journal (May 26, 2020); *Facebook Knew Calls For Violence Plagued 'Groups,' Now Plans Overhaul*, Wall Street Journal (Jan. 31, 2020); *Twitter Suspends More Than 50 White Nationalist Accounts*, NBC News (July 10, 2020); *Twitter Still Has A White Nationalist Problem*, HuffPost (May 30, 2019); Cornell University, *Auditing Radicalization Pathways On YouTube* (Dec. 4, 2019).

[18] Federal Bureau of Investigation, What We Investigate (www.fbi.gov/investigate/terrorism).

[19] *Democratic Senators Urge Facebook, Google and Twitter to Crack Down on Vaccine Misinformation*, CNBC (Jan. 25, 2021); *COVID Vaccine: Disappearing Needles and Other Rumors Debunked*, BBC News (Dec. 20, 2020); *Normalization of Vaccine Misinformation on Social Media Amid COVID 'a Huge problem,'* ABC News (Dec. 10, 2020); '*We Are Talking About People's Lives': Dire Warnings of Public Health Crisis as COVID-19 Misinformation Rages*, USA Today (Dec. 9, 2020); *Misinformation Messengers Pivot from Election Fraud to Peddling Vaccine Conspiracy Theories,* New York Times (Dec. 16, 2020); *Surge of Virus Misinformation Stumps Facebook and Twitter*, New York Times (Mar. 8, 2020).

[20] *The Propaganda Tools Used by Russians to Influence the 2016 Election*, New York Times (Feb. 16, 2018).

[21] *'Not A Whole Lot Of Innovation': 2020 Election Misinformation Was Quite Predictable, Experts Say*, USA Today (Nov. 17, 2021); *Did Social Media Actually Counter Election Misinformation?*, Associated Press, (Nov. 4, 2020).

engages users and so this type of content is prioritized, leading to rampant misinformation and conspiracies and, in turn, increased anger, hate, and intolerance, both online and offline."[22]

Through letters and hearings, the members of this Committee have appealed to many social media platforms to take actions to limit the spread of harmful content.[23] Since the 115th Congress,

---

[22] House Committee on Energy and Commerce, Testimony of Dr. Hany Farid, Professor, University of California, Berkeley *Hearing on A Country in Crisis: How Disinformation Online is Dividing the Nation*, 116th Cong. (June 24, 2020). *See also* Keach Hagey, *Facebook Tried To Make Its Platform a Healthier Place. It Got Angrier Instead*, Wall Street Journal (Sept. 15, 2021) (www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215?mod=article_inline).

[23] *See, e.g.*, House Committee on Energy and Commerce, *Hearing on Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation*, 117th Cong. (Mar. 25, 2021); Letter from Rep. Frank Pallone, Jr., Chairman, House Committee on Energy and Commerce, Rep. Mike Doyle, Chairman, Subcommittee on Communications and Technology, and Rep. Jan Schakowsky, Chair, Subcommittee on Consumer Protection and Commerce, to Mr. Sundar Pichai, CEO, Google (Mar. 3, 2021); Letter from Rep. Frank Pallone, Jr., Chairman, House Committee on Energy and Commerce, Rep. Diana DeGette, Chair, Subcommittee on Oversight and Investigations, Rep. Mike Doyle, Chairman, Subcommittee on Communications and Technology, and Rep. Jan Schakowsky, Chair, Subcommittee on Consumer Protection and Commerce, to Mr. Mark Zuckerberg, Chairman and CEO, Facebook (Feb. 23, 2021); Letter from Rep. Frank Pallone, Jr., Chairman, House Committee on Energy and Commerce, Rep. Anna G. Eshoo, Chairwoman, Subcommittee on Health, Rep. Diana DeGette, Chair, Subcommittee on Oversight and Investigations, Rep. Mike Doyle, Chairman, Subcommittee on Communications and Technology, and Rep. Jan Schakowsky, Chair, Subcommittee on Consumer Protection and Commerce, to Mr. Sundar Pichai, CEO, Google (Feb. 2, 2021); Letter from Rep. Frank Pallone, Jr., Chairman, House Committee on Energy and Commerce, Rep. Anna G. Eshoo, Chairwoman, Subcommittee on Health, Rep. Diana DeGette, Chair, Subcommittee on Oversight and Investigations, Rep. Mike Doyle, Chairman, Subcommittee on Communications and Technology, and Rep. Jan Schakowsky, Chair, Subcommittee on Consumer Protection and Commerce, to Mr. Mark Zuckerberg, Chairman and CEO, Facebook (Feb. 2, 2021); Letter from Rep. Frank Pallone, Jr., Chairman, House Committee on Energy and Commerce, Rep. Anna G. Eshoo, Chairwoman, Subcommittee on Health, Rep. Diana DeGette, Chair, Subcommittee on Oversight and Investigations, Rep. Mike Doyle, Chairman, Subcommittee on Communications and Technology, and Rep. Jan Schakowsky, Chair, Subcommittee on Consumer Protection and Commerce, to Mr. Jack Dorsey, CEO, Twitter (Feb. 2, 2021); House Committee on Energy and Commerce, *Hearing on Mainstreaming Extremism: Social Media's Role in Radicalizing America*, 116th Cong. (Sept. 21, 2020); House Energy and Commerce Committee, *Hearing on A Country in Crisis: How Disinformation Online is Dividing the Nation*, 116th Cong. (June 24, 2020); House Committee on Energy and Commerce, *Hearing on Fostering a Healthier Internet to Protect Consumers*, 116th Cong. (Oct. 16, 2019); Letter from Rep. Frank Pallone, Jr., Ranking Member, House Committee on Energy and Commerce, to Mr. Larry Page, CEO, Alphabet, Inc.; Mr. Mark Zuckerberg, CEO, Facebook, Inc.; and Mr. Jack Dorsey, CEO, Twitter, Inc. (Oct. 4, 2018); House Committee on Energy and Commerce, *Hearing on Facebook: Twitter: Transparency and Accountability*, 115th Cong. (Sept. 5, 2018); House Committee on Energy and Commerce, *Hearing on Facebook: Transparency and Use of Consumer Data*, 115th Cong. (Apr. 11, 2018); Letter from Rep. Frank Pallone, Jr., Ranking Member, House Committee on Energy and Commerce, to Mr. Larry Page, CEO, Alphabet, Inc.;

the Committee on Energy and Commerce has held six hearings examining the immunity protections in Section 230 of the Communications Decency Act (CDA 230), social media platform practices, and associated harms. The full Committee held a joint hearing on March 11, 2018, to review Facebook's use of consumer data[24] and on September 5, 2018, to review Twitter's algorithms and content moderation practices.[25] In the 116th Congress, the Subcommittee on Communications and Technology (CAT) and the Subcommittee on Consumer Protection and Commerce (CPC) held joint hearings on fostering a healthier internet[26] and disinformation,[27] and the CPC subcommittee held a hearing examining social media's role in fostering radical extremism.[28] Most recently, in March 2021, the CAT and CPC subcommittees held a hearing with the Chief Executive Officers of the biggest social media platforms.[29] Over the course of these hearings, members of the Committee warned that Congress would have to take legislative action if the platforms did not self-regulate.[30]

C. Original and Statutory Text of Section 230

Congress enacted CDA 230 in 1996 in part to help address the challenges early online platforms, such as message boards, faced in addressing harmful content on their services.[31] CDA 230 was enacted in the wake of a particular case, *Stratton-Oakmont, Inc. v. Prodigy Services Co*.[32] In that case, the New York Supreme Court was asked whether a website, Prodigy, could be held liable as a publisher when it actively used "technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and 'bad taste.'"[33] There, a user of one of

---

Mr. Mark Zuckerberg, CEO, Facebook, Inc.; and Mr. Jack Dorsey, CEO, Twitter, Inc. (Oct. 23, 2017).

[24] House Committee on Energy and Commerce, *Hearing on Facebook: Transparency and Use of Consumer Data*, 115th Cong. (Apr. 11, 2018).

[25] House Committee on Energy and Commerce, *Hearing on Facebook: Twitter: Transparency and Accountability*, 115th Cong. (Sept. 5, 2018).

[26] House Committee on Energy and Commerce, *Hearing on Fostering a Healthier Internet to Protect Consumers*, 116th Cong. (Oct. 16, 2019).

[27] House Committee on Energy and Commerce, *Hearing on A Country in Crisis: How Disinformation Online is Dividing the Nation*, 116th Cong. (June 24, 2020).

[28] House Committee on Energy and Commerce, *Hearing on Mainstreaming Extremism: Social Media's Role in Radicalizing America*, 116th Cong. (Sept. 21, 2020).

[29] House Committee on Energy and Commerce, *Hearing on Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation*, 117th Cong. (Mar. 25, 2021).

[30] *See* notes 24-29.

[31] *See e.g.,* 47 U.S.C. § 230(b)(4).

[32] Electronic Frontier Foundation, *CDA 230: Legislative History* (https://www.eff.org/issues/cda230/legislative-history).

[33] *Stratton Oakmont Inc. v. Prodigy Services Company*, 1995 WL 323710 (N.Y. Sup. Ct. 1995). *See also* Memorandum from Chairman Pallone to the Subcommittee on Communications and Technology and the Subcommittee on Consumer Protection and Commerce, Hearing on Fostering a Healthier Internet to Protect Consumers (Oct. 16, 2019).

Prodigy's bulletin boards had claimed Stratton Oakmont—the Long Island, NY investment firm depicted in the 2013 film the Wolf of Wall Street—had committed criminal acts. Stratton Oakmont sued the website—Prodigy—as the publisher of defamatory material. The court agreed that Prodigy could be determined to be liable as the publisher of that content, holding that "Prodigy's conscious choice to gain the benefits of editorial control, has opened it up to a greater liability."[34]

Congress responded by passing CDA 230. In particular, subsection (c)(1) of CDA 230 provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[35] Separately, subsection (c)(2) provides that:

> No provider or user of an interactive computer service shall be held liable on account of—
>
> **(A)**
> 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; or
>
> **(B)**
> any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

In passing CDA 230, Congress devised and incorporated statements of United States policy into the legislation to, among other things, "preserve the vibrant and competitive free market that presently exists for the internet and other interactive computer services." Congress similarly noted that it is the policy of the United States to "encourage the development of technologies which maximize user control of what information is received by individuals, families, and schools, who use the internet and other interactive computer services."[36]

Neither CDA 230 subsection (c)(1) or (c)(2) gives a platform immunity for content that the platform itself creates.[37] CDA 230(c)(2) grants immunity for actions taken in "good faith," to limit the reach of content, which makes this section's immunity narrower than Section 230(c)(1), which has been interpreted to offer immunity for removing *and* keeping up content. CDA 230(c) generally speaking has been interpreted not to solely immunize websites from third-party content posted on their sites, but it also often immunizes websites from their own decisions to remove objectionable content and their own decisions about how to structure their sites or applications.

---

[34] *Id.*

[35] 47 U.S.C. § 230(c)(1).

[36] 47 U.S.C. § 230 (b).

[37] 47 U.S.C. § 230 (c)(1).

Courts have reinforced that websites are eligible for CDA 230 immunity when screening or blocking content.[38]

Beyond the scope of the statutory text in subsection (c)(1) and (c)(2), CDA 230 also includes several explicit exemptions. Under those exemptions, platforms may still be held liable for third-party content that violates: (1) federal criminal law; (2) intellectual property law; (3) the Electronic Communications Privacy Act; and (4) certain laws relating to the promotion or facilitation of prostitution or sex trafficking.[39]

D. Amendment to Section 230—SESTA/FOSTA

Congress has only revised the scope of CDA 230 immunity once since its original passage and that was as part of the Allow States and Victims to Fight Online Sex Trafficking Act of 2017—often referred to as SESTA/FOSTA.[40] By amending Title 18 of the U.S. Code and CDA 230, that law enabled victims and their legal representatives to file private civil suits against persons or organizations that promote or facilitate prostitution or sex trafficking—broadly speaking.[41] As part of that, SESTA/FOSTA established criminal penalties for those who promote or facilitate prostitution and sex trafficking through their ownership, management, or operation of online platforms.[42] Notably, while the title of this law speaks only to sex trafficking, the text explicitly criminalizes, and provides a new civil remedy, in cases where consensual but illegal acts of prostitution or sex work are facilitated by websites.[43]

Since its passage, SESTA/FOSTA has been criticized as making sex workers less safe in that through providing civil and criminal penalties for websites that host illegal prostitution, sex workers were forced into more dangerous situations.[44] According to the Government Accountability Office (GAO), "[a]s of March 2021, [the Department of Justice] had brought one case under the criminal provision established by section 3 of [SESTA/]FOSTA for aggravated violations involving the promotion of the prostitution of five or more persons, or acting in reckless

---

[38] Memorandum from Chairman Pallone to the Subcommittee on Communications and Technology and the Subcommittee on Consumer Protection and Commerce, Hearing on Fostering a Healthier Internet to Protect Consumers (Oct. 16, 2019).

[39] 47 U.S.C. § 230(e).

[40] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164 (2018).

[41] *Id*. ((notably, Congress amended CDA 230 in 1998, but only to add an obligation to interactive computer services, not to limit or broaden the scope of the immunity granted under subsection (c)(1) and (c)(2)).

[42] *See* 18 U.S.C. § 2421A.

[43] *Id.*

[44] WHYY, *FOSTA-SESTA was supposed to thwart sex trafficking. Instead, it's sparked a movement* (July 10, 2020) (whyy.org/segments/fosta-sesta-was-supposed-to-thwart-sex-trafficking-instead-its-sparked-a-movement/).

disregard that conduct contributes to sex trafficking."[45] Similarly, GAO found that only one civil case was brought under Section 3 of SESTA/FOSTA but the case was dismissed.[46] Notably, however, GAO did not conclude an exhaustive review of the cases brought under section 4 of SESTA/FOSTA, which, still require that there be a violation of section 3 to proceed, or one of two other preexisting federal criminal laws related to sex trafficking.

E. Section 230's Application in Federal Courts

To begin, in federal courts CDA 230 immunity is generally raised at the initial motion to dismiss stage for failure to state a claim.[47] At this stage of litigation, an individual bringing a case against a platform for a claim arising from harm caused by the platform is generally not yet entitled to discovery.[48] Even where discovery might be available at this stage, courts routinely agree to stay (*i.e.,* stop) discovery at the request of platforms. Deciding CDA 230 immunity at this initial stage of litigation, without an opportunity for discovery, contributes to the lack of transparency of online platform operations as does the wholesale dismissal of individual claims without any consideration of the claims' merits. At the same time, by dismissing claims at such an early stage, litigants are spared from the more costly parts of litigation.[49]

F. Selected Significant Judicial Interpretations of Section 230

Since its passage, courts have been asked to apply CDA 230's liability protection in myriad different circumstances, and courts have generally read the provisions to apply broadly to a range of activities conducted by social media platforms.[50] The majority of CDA 230 cases deal with (c)(1), which the courts have, through years of cases, generally interpreted to extend broad

---

[45] Government Accountability Office, *Sex Trafficking: Online Platforms and Federal Prosecutions* (June 2021) (GAO-21-385).

[46] *Id*.

[47] *See, e.g.*, *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093 (9th Cir. 2019).

[48] *See* Fed. R. Civ. Pro. 12(b) ("A motion asserting any of these defenses must be made before pleading if a responsive pleading is allowed. If a pleading sets out a claim for relief that does not require a responsive pleading, an opposing party may assert at trial any defense to that claim. No defense or objection is waived by joining it with one or more other defenses or objections in a responsive pleading or in a motion").

[49] *Herrick v. Grindr, Inc.*, Petition for a Writ of Certiorari to the Supreme Court of the United States (plaintiff Herrick alleged the dating app Grindr should be held liable for claims resulting from a fake profile that led to hundreds of strange men coming to his home looking for sex and drugs; the Second Circuit Court of Appeals found that Grindr was immune from liability under CDA 230 and dismissed Herrick's claims without considering their merit); *See also* Eric Taubel, Note: *The ICS Three-Step: A Procedural Alternative for Section 230 of the Communications Decency Act and Derivative Liability in the Communications Decency Act and Derivative Liability in the Online Setting Online Setting*, Minnesota Journal of Law, Technology, and Policy, Vol. 12, Issue 1, Article 13 (2011).

[50] Congressional Research Service, *Section 230: An Overview*, R46751 (Apr. 7, 2021).

immunity to interactive computer services.[51] To benefit from CDA 230(c)(1)'s immunity, courts have applied a three-part test: (1) the platform must be a "provider or user of an interactive computer service," (2) which the plaintiff is treating as a "publisher or speaker" of (3) content "provided by another information content provider."[52] Courts have construed the definition of "interactive computer service" fairly comprehensively, so the success of a (c)(1) motion often depends on whether the other two conditions have been satisfied.[53]

In determining whether a platform should be treated as a "publisher or speaker" courts often look to the decision by the U.S. Court of Appeals for the Fourth Circuit in *Zeran v. America Online*.[54] Zeran sued America Online (AOL) after an anonymous individual posted a message about the sale of shirts featuring offensive slogans about the Oklahoma City Bombing on an AOL bulletin board.[55] The posts indicated that anyone interested in buying the shirts should call Zeran's telephone number, a number Zeran used to operate a business out of his home. Zeran began receiving a deluge of harassing phone calls, including death threats, and informed AOL.[56] The company said it would remove the post. Additional new posts with similar messages over the following four days, and the number of threatening calls intensified. Zeran called the Federal Bureau of Investigation and his local police. Once media in Oklahoma City began reporting that the posts were a hoax, the number of calls subsided.[57] Zeran sued AOL, arguing that once the company was made aware of the harmful third-party content, it had a duty to remove the post promptly, to notify subscribers that it was fake, and to screen future defamatory material.[58] In finding that AOL was a publisher of the content, and dismissing the suit, the court determined that Section 230(c)(1) bars "lawsuits seeking 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."[59] Further, the *Zeran* court found that section (c)(1) also bars the imposition of distributor liability as "merely a subset, or a species, of publisher liability, and

---

[51] *See, e.g., Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998); *Zeran v. AOL*, 129 F.3d 327 (4th Cir. 1997).

[52] *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100-01 (9th Cir. 2009).

[53] *Jones v. Dirty World Ent. Recordings LLC*, 755 F.3d 398, 406 n.2 (6th Cir. 2014) (observing that the term "interactive computer service" covers "broadband providers, hosting companies, and website operators").

[54] *Zeran v. America Online,* 129 F.3d 327, 330 (4th Cir. 1997).

[55] *Id*. at 329.

[56] *Id*.

[57] *Id*.

[58] *Id*. at 330.

[59] *Id*. at 330 (The court stated that "[p]ublishers can be held liable for defamatory statements contained in their works even absent proof that they had specific knowledge of the statement's inclusion") (quoting W. Page Keeton, et. Al., *Prosser and Keeton on the Law of Torts* §331 at 810). *See also Hassell v. Bird*, 420 P.3d 776, 789 (Cal. 2018); *Jones*, 755 F.3d at 407; *Barnes*, 570 F.3d at 1102.

therefore also foreclosed."[60]

Many other CDA 230 cases turn on the third prong of the test: whether the content in question is provided by another information content provider. An "information content provider" is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the internet or any other interactive computer service."[61] The U.S. Court of Appeals for the Ninth Circuit (Ninth Circuit) in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC* interpreted this definition to find that a platform could be considered an information content provider.[62] At issue in this appeal was whether Roommates.com could be sued under federal and state fair housing laws for asking its users about their sex, sexual orientation, whether they have children, and their preferences for these characteristics in a roommate.[63] The court found that Roommates.com "created" content when it created and required users to answer a questionnaire with choices provided by Roommates.com, and further, that Roommates.com "developed" content by designing a search system that "would steer users based on the preferences and personal characteristics that Roommate itself force[d] subscribers to disclose."[64] However, the Court limited the reach of its holding by specifying that as long as a platform provides "neutral tools" for users to post content on the platform or perform a search using user-generated criteria, that would not constitute developing content, and that "development" as used in Section 230 means "materially contributing to its alleged unlawfulness."[65]

Plaintiffs have tried, mostly unsuccessfully, to argue that the use of algorithms to curate the third-party information presented to users turns social media platforms into information content providers rather than mere publishers of third-party content. Courts that have considered this argument have grounded their rejection of the plaintiffs' claims, and the application of CDA 230 immunity, using the "neutral tools" and "material contribution" reasoning from *Roommates.com*.[66]

---

[60] *Zeran* at 332 (Citing *Prosser and Keeton on the Law of Torts*, the court explained that "[d]istributors cannot be held liable for defamatory statements contained in the materials they distribute unless it is proven at a minimum that they have actual knowledge of the defamatory statements upon which liability is predicated." *Zeran a*t 331.)

[61] 47 U.S.C. § 230(f).

[62] 521 F.3d 1157, 1168 (9th Cir. 2008). *See also*, *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1199 (10th Cir. 2009) (in a case involving a website that obtained private telephone records, the Tenth Circuit followed the rule and reasoning in *Roommates.com* in holding that a party is "responsible" for content only when the party "in some way specifically encourages development of what is offensive about the content.").

[63] *Id*. at 1166-1167.

[64] *Id*. at 1164-68.

[65] *Id*. at 1167–69.

[66] *See, e.g.*, *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1098-1099 (9th Cir. 2019) (plaintiffs could not frame "website features as content" and the platform's recommendation and notification functions did not materially contribute to alleged unlawfulness of content); *Force v. Facebook*, 934 F.3d at 66–69 (rejecting theories that algorithmic sorting rendered website a non-publisher or materially contributed to development of content); *Marshall's Locksmith Serv.*, 925 F.3d 1263, 1271 (declining to treat search engines' conversion of fraudulent addresses from webpages into "map

For example, in *Marshall's Locksmith Service v. Google*, several locksmith businesses sued companies with search engines over their use of automated algorithms to amplify "scam" locksmith services, including scam addresses that are converted into "pinpoints" appearing on the search engines' mapping websites. The plaintiff locksmith firms claimed economic loss from these scam locksmith services. Plaintiffs claimed also, among other things, that the search engines' amplification and manipulation of the scam information—most notably in the pinpoint map of the service locations—turned the information posted by the scam business into new content. The U.S. Court of Appeals for the D.C. Circuit determined that the algorithms were a "neutral means" by which all types of information, including scam information, were translated in the same manner, thus the map pinpoints were protected by CDA 230.[67]

Similarly, in *Dyroff v. Ultimate Software Grp., Inc*., a social networking platform, Experience Project, allowed users to anonymously share first-person experiences on a variety of topics with other users.[68] This platform included a number of topics and forums, including "I like Dogs" and "I Go to Stanford" and "I like Heroin".[69] Experience Project used algorithms to analyze posts and other user data to make content recommendations and notifications to members of discussion groups, including groups that discussed and facilitated illegal drug sales. Plaintiff Dyroff sued the Ultimate Software Group after her son died from an overdose after soliciting and purchasing fentanyl-laced heroin from another user.[70] Dyroff's son was a member of a heroin-related group on the platform and asked other users of the group where he could purchase drugs in his area. The platform sent him an email when another user in the group responded to his inquiry, and the two met off-line for the drug purchase. The U.S. Court of Appeals for the Ninth Circuit found that the platform was entitled to CDA 230 immunity under section (c)(1) because the platform's "content-neutral tools"—recommendation and notification functions—facilitated communication but did not materially contribute to the alleged unlawfulness of the content.[71]

In *Force v. Facebook*, victims of terrorist attacks committed by Hamas alleged that Facebook unlawfully provided Hamas with a communications platform that enabled Hamas's terrorist attacks. Plaintiffs alleged that Facebook either was not acting as a publisher because Facebook's algorithms directed personalized content and friend suggestions to users who would be most interested in Hamas's activities or, alternatively, Facebook materially contributed to the development of user content by making Hamas's content more "visible, available, and usable."[72] The U.S. Court of Appeals for the Second Circuit rejected this argument by the plaintiffs and determined that Facebook was entitled to CDA 230 immunity because Facebook was acting as the publisher of information and was not an information content provider because Facebook's "arranging and distributing of third-party information… is an essential result of publishing," whether or not algorithms are used, and Facebook's recommendation algorithms were content

---

pinpoints" as developing content).

[67] *Marshall's Locksmith Serv.*, 925 F.3d at 1271.

[68] *Dyroff*, 934 F.3d at 1094.

[69] *Id*.

[70] *Id*. at 1095, 1098.

[71] *Id*. at 1096, 1099.

[72] *Force*, 934 F.3d at 66-70.

"neutral" and used "objective factors" that applied in the same way when displaying third-party content.[73] In a separate opinion, Judge Katzmann questioned "whether, and to what extent, Congress should allow liability for tech companies that encourage terrorism, propaganda, and extremism is a question for legislators, not judges. Over the past two decades 'the Internet has outgrown its swaddling clothes,' and it is fair to ask whether the rules that governed its infancy should still oversee its adulthood."[74]

The Ninth Circuit reached a similar conclusion in *Gonzalez v. Google, LLC*, a case brought by the families of victims of ISIS terrorist attacks.[75] The Gonzalez plaintiffs alleged Google provided "material support" to ISIS by allowing terrorists to use Google's platform as a tool to facilitate recruitment and commit terrorism.[76] The court found that Google did not act as an "information content provider" when using algorithms to recommend terrorist content because Google used a neutral algorithm that did "not treat ISIS-created content differently than any other third-party created content" and Google provided a "neutral platform" that did not encourage the posting of unlawful material.[77] However, in a separate opinion, one judge in the case questioned whether CDA 230's immunity had been properly interpreted by the courts, and called on Congress to clarify the law. Specifically, Judge Gould said, "if Congress continues to sleep at the switch of social media regulation in the face of courts broadening what appears to have been its initial and literal language and expressed intention under Section 230, then it must fall to the federal courts to consider rectifying those errors itself by providing remedies to those who are injured by dangerous and unreasonable conduct." A petition for rehearing en banc is currently pending in the case.

However, at least one case has suggested a limit to the "neutral tools" analysis. In *Lemmon v. Snap, Inc.*, the parents of teenagers who died in a fatal car accident sued Snap, Inc. after one of the teenagers used Snapchat's "Speed Filter" app to document how fast they were driving shortly before the accident.[78] The Ninth Circuit noted that it "has never suggested that internet companies enjoy absolute immunity from all claims related to their content-neutral tools."[79] The court determined that the plaintiffs' claims would not be barred by Section 230(c)(1) because Snapchat's speed filter neither treated the platform as a "publisher or speaker" nor relied on "information provided by another information content provider."[80] The court reasoned that this particular content created by Snapchat's users did not cause the harm, but that the existence of the speed filter

---

[73] *Id*. at 66-70.

[74] *Id*. at 77 (Katzmann, J., partial concurrence and partial dissent).

[75] *Gonzalez v. Google*, 2 F.4th at 871. This case deals with district court's dismissal of three actions seeking damages against Google, Twitter, and Facebook for allowing ISIS to communicate ISIS's message and to radicalize new recruits on their platforms. Only the Gonzalez case involved dismissal under CDA 230.

[76] *Id*. at 882.

[77] *Id*. at 894–96. However, claims that Google funneled a portion of its advertising revenue to ISIS-related content used to recruit new ISIS volunteers was not immune under CDA 230.

[78] *Lemmon v. Snap, Inc.*, 995 F.3d 1085 (9th Cir. 2021).

[79] *Id*. at 1094.

[80] *Id*. at 1091-1094.

itself encouraged Snapchat's users to speed.[81] Further, the court observed that the lawsuit sought to hold Snap liable for its "unreasonable and negligent" design decisions regarding Snapchat.[82]

Notably, some courts have limited the reach of (c)(1)'s protections in the case of platforms that are online marketplaces. In *Oberdorf vs. Amazon*, Amazon asserted a defense under section (c)(1) when a plaintiff sued the company for a defective dog collar she purchased on its website left her permanently blind in one eye.[83] Oberdrof's claims against Amazon included liability for negligence such as failure to warn and strict liability. Amazon claimed that CDA 230 barred Oberdorf's claims because she sought to treat the company as a publisher or speaker of the third-party content provided by the manufacturer of the defective collar. In its opinion partially granting and partially denying the CDA 230 defense, the U.S. Circuit Court for Third Circuit differentiated between the claims that sought to hold Amazon liable as seller of the defective product, and the claims that sought to hold Amazon responsible for the content of the listing on its website. The court held that CDA 230 protected Amazon for the latter but said CDA 230 did not protect Amazon as the seller and distributor of the product.

II. LEGISLATION

A. H.R. 2154, the "Protecting Americans from Dangerous Algorithms Act"

H.R. 2154, the "Protecting Americans from Dangerous Algorithms Act," introduced by Reps. Malinowski (D-NJ) and Eshoo (D-CA), would amend section (c)(1) of CDA 230 to preclude an interactive computer service from claiming immunity in instances where it uses an algorithm to amplify or recommend content directly relevant to a case involving interference with civil rights, neglect to prevent interference with civil rights, and in cases revolving international terrorism. However, the platform could regain the liability restrictions if it makes the operation of its algorithm "obvious, understandable, and transparent to a reasonable user," or in cases where a platform provides an algorithm to support search features that users voluntarily opt to use.

B. H.R. 3184, the "Civil Rights Modernization Act of 2021"

H.R. 3184, the "Civil Rights Modernization Act of 2021," introduced by Rep. Clarke (D-NY), would amend section 230(e), which provides exemptions to the Section 230(c) protections, for the targeting of ads where such ads violate civil rights laws. Civil rights laws include federal, state, and local laws that prohibit discrimination on the basis of a protected class or status or prohibit voter access.

C. H.R. 3421, the "Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act" or the "SAFE TECH Act"

H.R. 3421, the "SAFE TECH Act," introduced by Reps. McEachin (D-VA), Castor (D-FL) and Levin (D-CA), would reform Section 230 by (1) replacing immunity under (c)(1) for third party "information" with immunity for third-party "speech"; (2) removing Section 230 protections

[81] *Id.* at 1094.

[82] *Id.* at 1091.

[83] *Oberdorf v. Amazon.com, Inc.*, 930 F.3d 136 (3rd Cir. 2019).

for paid advertisements; (3) prohibiting interactive computer service from pleading immunity under CDA 230 in requests for injunctive relief in certain cases; and (4) creating additional immunity exemptions for state or federal civil rights laws, state or federal antitrust laws, state or federal stalking or harassment laws, international human rights laws, and wrongful death actions. A companion bill was introduced by Senators Warner (D-VA), Hirono (D-HI) and Klobuchar (D-MN).[84]

D. H.R. 5596, the "Justice Against Malicious Algorithms Act"

H.R. 5596, the "Justice Against Malicious Algorithms Act of 2021," introduced by Reps. Pallone (D-NJ), Doyle (D-PA), Schakowsky (D-IL), and Eshoo (D-CA) would amend CDA 230 to remove absolute immunity in certain instances. Specifically, the bill would lift the liability shield in section (c)(1) of CDA 230 when an online platform knowingly or recklessly uses an algorithm to recommend content that materially contributes to physical or severe emotional injury. The bill includes exceptions, thus leaving the CDA 230 (c)(1) immunity intact, for user-generated search, internet infrastructure such as web hosting or data storage and transfer, and for small online platforms with fewer than five million unique monthly visitors or users.

III. WITNESSES

The following witnesses have been invited to testify:

Panel I

Frances Haugen
Former Facebook Employee

Rashad Robinson
President
Color of Change

James Steyer
Founder and CEO
Common Sense Media

Kara Frederick
Research Fellow in Technology Policy
The Heritage Foundation

Panel II

The Honorable Karen Kornbluh
Director, Digital Innovation and Democracy Initiative and Senior Fellow
The German Marshall Fund of the United States

[84] S. 299.

Carrie Goldberg, Esq.
Owner
C. A. Goldberg Law Firm, PLLC

Matthew F. Wood
Vice President of Policy and General Counsel
Free Press Action

Dr. Mary Anne Franks
Professor of Law and Michael R. Klein Distinguished Scholar Chair, University of Miami School of Law
President and Legislative & Tech Policy Director, Cyber Civil Rights Initiative

Eugene Volokh
Gary T. Schwartz Distinguished Professor of Law
UCLA School of Law

Daniel A. Lyons
Professor & Associate Dean for Academic Affairs, Boston College Law School
Nonresident Senior Fellow, American Enterprise Institute