Western New England Law Review

Volume 44 *44*
Issue 1

Article 2

2022

THE BIG TECH ACCOUNTABILITY ACT: REFORMING HOW THE BIGGEST CORPORATIONS CONTROL AND EXPLOIT ONLINE COMMUNICATIONS

Ben Clements

WESTERN NEW ENGLAND LAW REVIEW

Volume 44 2022 Symposium

THE BIG TECH ACCOUNTABILITY ACT: REFORMING HOW THE BIGGEST CORPORATIONS CONTROL AND EXPLOIT ONLINE COMMUNICATIONS

BEN CLEMENTS*

INTRODUCTION

A handful of global corporations have taken control of the internet, the dominant medium of modern communication and commerce, and have used that control to create and sell databases of personal information of Americans and to systematically amplify dangerous disinformation and violence on an unprecedented scale. This has created a growing threat to our democracy and our people.

While our elected officials and many in the media claim to recognize the danger, a corporate-friendly First Amendment absolutism and misguided fears about chilling voices on the internet have preempted any serious effort at reform or regulation. Neither the First Amendment nor the desire to protect the robust exchange of ideas on the internet justifies this inaction. Instead, legislation that would protect personal privacy and autonomy on the internet and hold Big Tech companies accountable for promoting fraudulent disinformation and violence would be consistent with the First Amendment and would, in fact, strengthen the free exchange of ideas on the internet.

Section I of this Article explains how the highly profitable Big Tech business model is built on exploiting individual privacy and autonomy at great risk to our democracy and public welfare and how Congress has failed to take any meaningful action to address this threat. Section II provides a summary of a legislative solution—the proposed Big Tech Accountability Act—that would hold Big Tech companies accountable for the substantial public harm that they cause, without violating anyone's

* Ben Clements is an attorney, author, and advocate for political and governmental reform, and serves as the chairman and senior legal advisor of Free Speech For People, a national non-profit organization defending our democracy and challenging corruption and abuse of corporate power.

First Amendment rights. Section III summarizes and rebuts the common First Amendment, and other, objections to imposing liability on social media companies. Finally, the Article concludes with the full text of the proposed Big Tech Accountability Act.

I. THE URGENT NEED TO HOLD BIG TECH ACCOUNTABLE

In recent years, global technology companies—often known as "Big Tech"—and specifically the biggest social media companies, have emerged as perhaps the biggest corporate threat to our constitutional democracy. They have mastered the corporate playbook of using a combination of big-money lobbying, massive campaign spending, and heavily funded propaganda campaigns to deter and prevent any meaningful government regulation; to facilitate unprecedented monopolistic growth; and to ensure that they continue to enjoy immunity from legal accountability[1] that has never been available to other communications companies, whether print or broadcast. And they have built a multi-billion-dollar business model that profits from exploiting and selling the personal information of virtually every American and facilitating and promoting disinformation and violence that undermine our democracy, our healthcare, our civil rights, and our capacity for rational self-government.

The result has been colossal wealth for the Big Tech companies and their owners, but at the expense of the autonomy and privacy of most Americans, and at great risk to our democracy and our individual and collective welfare. The Big Tech business model, which thrives on promoting the most sensational—and generally false—material through the use of highly efficient algorithms, has caused or contributed to a staggering array of serious public harm, including physical and psychological disorders[2] and suicidal ideation among young people;[3] the inability to effectively address major healthcare issues,[4] including the

1. 47 U.S.C. § 230.

2. *E.g.*, Georgia Wells et al., *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J. (Sept. 14, 2021, 7:59 AM), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739 [https://perma.cc/L3JD-7DEG].

3. Karen Feldscher, *How Social Media's Toxic Content Sends Teens into 'A Dangerous Spiral'*, HARV. T.H. CHAN (Oct. 8, 2021), https://www.hsph.harvard.edu/news/features/how-social-medias-toxic-content-sends-teens-into-a-dangerous-spiral/ [https://perma.cc/R3DL-DT2E]; Ysabel Gerrard & Tarleton Gillespie, *When Algorithms Think You Want to Die*, WIRED (Feb. 21, 2019, 12:41 PM), https://www.wired.com/story/when-algorithms-think-you-want-to-die/ [https://perma.cc/XB6Z-DTAC].

4. *See* Victor Suarez-Lledo & Javier Alavrez-Galvez, *Prevalence of Health Misinformation on Social Media: Systematic Review*, 23 J MED. INT. RSCH., no. 1, 2021, at 1, https://www.jmir.org/2021/1/e17187/PDF [https://perma.cc/RMT9-ZEYG].

COVID-19 pandemic;[5] facilitating sexual predation and exploitation;[6] violence and genocide;[7] interfering with free and fair elections;[8] and inciting a violent insurrection at the United States Capitol.[9] Despite growing public concern and the highly publicized shows of outrage from our politicians, Congress has failed to take any meaningful action.

Every few months, in the face of the latest revelations of abuses, Congress holds show hearings and invites the Big Tech executives to appear.[10] Members of Congress use these hearings to publicly condemn the Big Tech companies and their top executives and to threaten some unspecified action. But the action never materializes. Instead, the congressional hearings end up serving as a platform for the Big Tech executives to offer misleading defenses and walk away with empty reassurances about how hard they are trying to protect us[11] from the venom that they are in fact actively promoting on their platforms.

For example, recent revelations from Facebook (now Meta) whistleblowers indicate that while Facebook executives publicly claim that they are seeking to combat harmful content on their platforms, they have in fact knowingly allowed it to flourish. "Facebook, over and over

5. Terry Collins, *'This Deception Must End Now': Facebook Gets Letter from 500 Health Professionals Demanding Data on COVID Misinformation*, USA TODAY (Nov. 5, 2021, 11:53 PM), https://www.usatoday.com/story/tech/2021/11/05/facebook-covid-misinformation-doctors-letter/6275730001/ [https://perma.cc/MG6A-AGN8].

6. Kari Paul, *Over 300 Cases of Child Exploitation Went Unnoticed by Facebook – Study*, GUARDIAN (Mar. 4, 2020, 6:00 AM), https://www.theguardian.com/technology/2020/mar/04/facebook-child-exploitation-technology [https://perma.cc/8SMK-MDV9].

7. *E.g.*, Paul Mozur, *A Genocide Incited on Facebook, With Posts from Myanmar's Military*, N.Y. TIMES (Oct. 15, 2018), https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html [https://perma.cc/HL5B-PRBG].

8. Geoffrey A. Fowler, *Twitter and Facebook Warning Labels Aren't Enough to Save Democracy*, WASH. POST (Nov. 9, 2020), https://www.washingtonpost.com/technology/2020/11/09/facebook-twitter-election-misinformation-labels/ [https://perma.cc/CMR7-W5H5].

9. Craig Timber et al., *Inside Facebook, Jan. 6 Violence Fueled Anger, Regret over Missed Warning Signs*, WASH. POST (Oct. 22, 2021, 7:36 PM), https://www.washingtonpost.com/technology/2021/10/22/jan-6-capitol-riot-facebook/ [https://perma.cc/3GKD-KXDC].

10. Tony Romm, *Amazon, Apple, Facebook and Google Grilled on Capitol Hill over Their Market Power*, WASH. POST (July 29, 2020), https://www.washingtonpost.com/technology/2020/07/29/apple-google-facebook-amazon-congress-hearing/ [https://perma.cc/FT8M-FHVF].

11. *See, e.g.*, Dean DeChiaro, *Social Media Algorithms Threaten Democracy, Experts Tell Senators*, ROLL CALL (Apr. 27, 2021, 3:08 PM), https://www.rollcall.com/2021/04/27/social-media-algorithms-threaten-democracy-experts-tell-senators/ [https://perma.cc/KP42-GU7T].

again, has shown it chooses profit over safety."[12] A pair of complaints filed with the Securities Exchange Commission in February 2022 allege, based on internal Facebook documents, that Facebook executives made false assurances to the public and members of the Senate about its purported efforts to combat climate change and COVID-19 disinformation, both of which continue to proliferate on their platforms.[13]

The Big Tech companies and their allies have been as successful at manipulating public discourse as they have been at neutering Congress. There is little discussion about passing laws that would hold Big Tech companies accountable for the massive public harm they cause. Instead, we buy into this fiction that any attempt to do so would violate the First Amendment. They have sold the public on the contradictory propositions that they cannot be held accountable for what third parties post on their platforms because it is the third parties and not the platforms that are doing the speaking and yet, at the same time, that it would violate the supposed free speech rights of the platforms to hold them accountable for speech that they insist they are not speaking.[14]

This propaganda doublespeak has been so effective that there is no serious effort to hold Big Tech platforms accountable for facilitating and amplifying disinformation and violence. Rather than regulating them like any other business, we treat the Big Tech companies like sovereign states, urging them to voluntarily introduce better oversight and moderating practices. But these pleas are destined to fail so long as these companies continue to profit without accountability from targeted amplification of disinformation, threats of violence, and other harmful conduct.

II. THE PROPOSED BIG TECH ACCOUNTABILITY ACT—SUMMARY

It does not have to be this way. Free Speech For People,[15] a national non-profit organization working to protect our constitutional democracy, has launched a campaign for legislative reform that would address the most serious damage caused by Big Tech social media companies. Constitutional lawyers at Free Speech For People have crafted model federal legislation, the Big Tech Accountability Act,[16] to hold social

12. Ryan Mac & Cecilia Kang, *Whistle-Blower Says Facebook 'Chooses Profits over Safety'*, N.Y. TIMES (Oct. 27, 2021), https://www.nytimes.com/2021/10/03/technology/whistle-blower-facebook-frances-haugen.html [https://perma.cc/F45Q-CJQJ].

13. Cat Zakrzewski, *Facebook Whistleblower Alleges Executives Misled Investors About Climate, Covid Hoaxes in New SEC Complaint*, WASH. POST (Feb. 18, 2022, 7:00 A.M.), https://www.washingtonpost.com/technology/2022/02/18/whistleblower-facebook-sec-climate-change/ [https://perma.cc/4SP2-SPMN].

14. *See infra* notes 23–24.

15. FREESPECHFORPEOPLE.ORG, https://freespeechforpeople.org/ [https://perma.cc/3KM6-Y98Y].

16. *The Big Tech Accountability Act*, FREESPEECHFORPEOPLE.ORG,

media companies accountable; to protect internet users, voters, and the broader community from the dangers of rampant amplification of disinformation and violence; and to protect online personal privacy and autonomy.

While the Big Tech Accountability Act addresses a wide range of threats posed by Big Tech, it does *not* rely on censorship by the government of either Big Tech companies or their users. Nor does it rely on the government mandating what content Big Tech companies should or should not screen or government mandates about whether and how to amplify or promote specific content. Instead, the Big Tech Accountability Act applies traditional and well-established legal principles for holding accountable persons or companies that make or promote fraudulent, false, and deceptive statements or statements made in a manner calculated to cause significant public harm and that promote violent criminal acts.

The Big Tech Accountability Act, the text of which is set forth in full below, has five key elements.[17] First, it would amend § 230 of the Communications Decency Act[18] to limit the blanket immunity of that section to internet platforms that do not in fact act as publishers. It would remove the immunity for internet companies that (a) engage in targeted amplification of content, (b) recklessly encourage or facilitate the spread of disinformation or violence, or (c) intentionally profit from amplifying disinformation or violence. This amendment would reinforce the original purpose of § 230 by preserving immunity for those companies that operate as passive platforms for users to post content, but it would level the playing field by treating those platforms that manipulate or target that content like any other publisher.

Second, the Act would ban "surveillance advertising,"[19] except for targeting of individuals based on geography and sorting for relevance based on individual search terms. While serving to reduce inequities and information distortion from targeting of content, this provision would also reduce the current incentives for Big Tech companies to collect and exploit people's personal data.[20]

Third, the Act would establish new federal criminal and civil liability

https://freespeechforpeople.org/wp-content/uploads/2022/01/big-tech-accountability-act_1_2022.pdf [https://perma.cc/2K4Y-PGFK]; *see also infra* pp. 13–28.

17. *See infra* pp. 13–28.

18. Communications Decency Act of 1996, 47 U.S.C. §§ 230, 560–61.

19. Accountable Tech defines "surveillance advertising" as "the practice of extensively tracking and profiling individuals and groups, and then microtargeting ads at them based on their behavioral history, relationships, and identity." Gilad Edelman, *This Group Wants to 'Ban Surveillance Advertising'*, WIRED (Mar. 22, 2021, 12:00 PM), https://www.wired.com/story/ban-surveillance-advertising-coalition-launches/ [https://perma.cc/R45U-MUMU].

20. Paul Jarvis, *We Must Ban Targeted Advertising Immediately*, FATHOM/ (Apr. 8, 2020), https://usefathom.com/blog/targeted-ads [https://perma.cc/NV6E-HAPN].

for knowingly disseminating fraudulent civic information, such as disinformation relating to voting, healthcare, or other essential government services, and for conducting targeted amplification of fraudulent civic information with reckless disregard for the risk of substantial public harm.

Fourth, the Act would establish new federal criminal and civil liability for engaging in targeted amplification of threats or solicitations to commit violent crimes—a provision modeled on existing federal law generally prohibiting the solicitation of violent crimes.

Finally, the Act would direct the Federal Trade Commission to make recommendations for prohibiting the aggregation and sale of personal information without informed and meaningful consent.

III. THE OBJECTIONS TO REGULATING BIG TECH DO NOT JUSTIFY INACTION

This section addresses the most common arguments made against accountability for social media companies. First, the argument that such accountability would violate the First Amendment is based on the mistaken assumption that accountability requires government "censorship." But the Big Tech Accountability Act would instead impose liability for amplifying fraudulent statements and encouragement of violence following well-established and permissible legal approaches. Second, contrary to the defenders of the status quo, continuing to immunize Big Tech from accountability hinders rather than promotes the free exchange of ideas on the internet. Third, existing laws are woefully inadequate to address the threats of amplified disinformation and violence, particularly while § 230 immunity remains in place. Fourth, holding Big Tech legally accountable would decrease, rather than increase, the risk of political and government manipulation of social media. Fifth, the answer to racial discrimination by the social media companies is not to continue immunizing them for the promotion of racist violence, but instead, to subject internet companies to the civil rights protections that already apply to other public accommodations. Finally, the fact that holding Big Tech companies accountable would require them to change their business models is an argument for, rather than against, accountability.

A. *First Amendment Objections to Holding Big Tech Accountable Are Unfounded*

It is widely assumed that government regulation to hold the big social media companies legally accountable for the content that they amplify on their platforms would run afoul of the First Amendment. To the extent that any reasoning is offered for this view, it typically rests on the notion that any effort to hold social media companies accountable would necessarily rely on government mandates or government "censorship" of

"false," or even merely objectionable, content.[21]

Contrary to these assumptions, the Big Tech Accountability Act does not give the government the power to mandate what or how internet companies choose to host or promote on their platform. Nor does it give the government any power to "censor" false, objectionable, or any other speech. It leaves the internet companies with the power that they currently have to make those decisions themselves. But when they choose to engage in promoting, amplifying, and targeting content, rather than simply acting as passive public forums, the Big Tech Accountability Act holds them accountable for substantial public harm caused by their promotion, amplification, or targeting of civic disinformation and solicitations to criminal violence.

There are several reasons that this approach does not run afoul of the First Amendment. As an initial matter, it is not clear that the Big Tech platforms, as distinct from their users, have any First Amendment interest in the content hosted on their platforms. Their favored argument against accountability—and the rationale behind the immunity they enjoy under § 230 of the Communications Decency Act[22]—is that they are neither the speaker nor the publisher of that content and therefore cannot be held accountable.[23] Indeed, the internet companies often insist that they cannot be accused of *intentionally* targeting and amplifying disinformation and violent content because they have no knowledge of the content and are unable (or unwilling) to monitor for such content.[24] But this claim does

21. *See* Nadine Strossen, *Disinfo v. Democracy*, TABLET (Sept. 19, 2021), https://www.tabletmag.com/sections/news/articles/disinformation-nadine-strossen [https://perma.cc/BKY8-YVQS].

22. 47 U.S.C. § 230.

23. For example, in *Gonzalez v. Google, LLC*, Google argued, and the Ninth Circuit agreed, that § 230 protected Google from liability for its role in promoting ISIS videos that helped lead to a massive deadly shooting in Paris, despite the fact that Google used algorithms to recommend the terrorist videos (on YouTube) to persons that Google determined were likely to respond favorably to them. Gonzalez v. Google, LLC, 2 F.4th 871, 894–95 (9th Cir. 2021). The court explained that, even though Google recommended the ISIS videos "based upon users' viewing history and what is known about the users," it did not create or develop the content, and therefore could not be held liable. *Id.* at 893–95. Other courts have likewise accepted these arguments on behalf of Big Tech companies. *See, e.g.*, Force v. Facebook, Inc., 934 F.3d 53, 68–71 (2d Cir. 2019) (adopting Facebook's argument that it was not the "creator or developer" of terrorist postings that Facebook recommended on its platform and therefore could not be liable for the resulting terrorist acts).

24. *See, e.g.*, *Hearing Before the United States House of Representatives Committee on Energy and Commerce Subcommittees on Consumer Protection & Commerce and Communications & Technology*, 117 Cong. 7 (2021), https://www.congress.gov/117/meeting/house/111407/witnesses/HHRG-117-IF16-Wstate-ZuckerbergM-20210325-U1.pdf [https://perma.cc/9EYG-QG9R] (testimony of Mark Zuckerberg, CEO, Facebook, Inc.) ("Platforms should not be held liable if a particular piece of content evades its detection—that would be impractical for platforms with billions of posts per day.").

not bring their actions within the protection of the First Amendment. To the contrary, it defeats any First Amendment defense: if they indeed have no knowledge of the content that they are amplifying, then they are engaged in purely transactional conduct, not expressive speech.

Even assuming, however, that internet companies have First Amendment interests in the content on their sites—either directly or on behalf of their users—the liability provisions of the Big Tech Accountability Act are fully consistent with the First Amendment.

While the First Amendment protects some "false" speech and the government may not pass a law simply banning whole categories of speech solely based on it being "false,"[25] the courts have long recognized that false speech that creates tangible public harm may properly be regulated. Perhaps the most famous example is the illustration provided by Justice Oliver Wendell Holmes: "The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic."[26] Thus, as the Supreme Court has recently recognized, false statements may properly form the basis for civil and criminal liability in cases involving "defamation, fraud, or some other legally cognizable harm associated with a false statement, such as an invasion of privacy or the costs of vexatious litigation."[27]

Indeed, *most* criminal laws (apart from those involving violent crime), especially at the federal level, hold people accountable for harmful false speech. For example, every criminal offense involving fraud, including insurance fraud,[28] bank fraud,[29] consumer fraud,[30] securities fraud,[31] and tax fraud[32]—even passing bad checks[33]—punishes people for false speech. Other examples include making false statements to the government,[34] falsifying documents or information in connection with a government investigation,[35] and perjury.[36] And on the civil side, there are

25. United States v. Alvarez, 567 U.S. 709 (2012).

26. Schenck v. United States, 249 U.S. 47, 52 (1919).

27. *Alvarez*, 567 U.S. 719.

28. FindLaw Staff, *Insurance Fraud*, FINDLAW, https://www.findlaw.com/criminal/criminal-charges/insurance-fraud.html [https://perma.cc/M4Y6-3JE2]; *see also* 18 U.S.C. § 1035.

29. 18 U.S.C. § 1344.

30. *See, e.g.*, *Types of Consumer Fraud*, OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/types-of-consumer-fraud.html [https://perma.cc/X4N8-GWQ2].

31. 18 U.S.C. § 1348.

32. 26 U.S.C. § 7206.

33. *E.g.*, Will Kenton, *Bad Check*, INVESTOPEDIA, https://www.investopedia.com/terms/b/bad-check.asp [https://perma.cc/SB5H-T8JU].

34. 18 U.S.C. § 1001.

35. 18 U.S.C. § 1505.

36. 18 U.S.C. § 1621.

numerous laws holding people accountable for harmful false speech, including libel and slander laws,[37] civil fraud laws,[38] unfair and deceptive practices laws,[39] and many more.

Nor does the First Amendment prevent the government from prohibiting making threats or solicitations of criminal acts of violence.[40] Many state and federal laws already prohibit threatening violence. An existing federal statute makes it a crime to solicit, induce, or persuade another to engage in criminal activity involving the use, attempted use, or threatened use of physical force against property or persons.[41] The Big Tech Accountability Act provision is modeled on that federal law and extends it to internet companies in circumstances in which they have engaged in targeting and amplification of the unlawful solicitations.

B. *Immunizing Big Tech from Accountability Does Not Promote Free Speech on the Internet*

Many continue to argue that internet companies must remain immune from accountability to ensure that their users are free to post whatever they want without the risk of screening, censoring, or manipulation by the internet companies.[42] Indeed, when the Communications Decency Act was passed in 1996, the idea behind immunity for internet companies was to enable online platforms to allow users to post content without risking liability for everything and anything that a user might choose to post.[43] But the big internet companies have long since stopped being passive platforms for people to post content; they instead play an active role in curating, amplifying, and targeting content—often illegal content—for their own profit. Contrary to its original purpose, § 230 of the Communications Decency Act now serves to protect massive targeting by the biggest platforms,[44] undermining the ability of ordinary people to

37. *E.g.*, *Defamation*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/defamation [https://perma.cc/S3R9-KC3A].

38. *E.g.*, *Fraud*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/fraud [https://perma.cc/559Y-JPBT].

39. 15 U.S.C. § 45.

40. "Speech integral to criminal conduct, such as fighting words, threats, and solicitations, remain categorically outside [First Amendment] protection." United States v. White, 610 F.3d 956, 960 (7th Cir. 2010) (citing United States v. Williams, 533 U.S. 285, 297 (2008); Bradenburg v. Ohio, 395 U.S. 444, 447–49 (1969)).

41. 18 U.S.C. § 373.

42. *E.g.*, Jason Kelley, *Section 230 Is Good, Actually*, EFF (Dec. 3, 2020), https://www.eff.org/deeplinks/2020/12/section-230-good-actually [https://perma.cc/8NVN-F4Q3].

43. Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14 (2020) (statement of Justice Thomas respecting the denial of certiorari) (summarizing the background and purpose of § 230 provisions).

44. *See id.* at 15–18 (summarizing the expansive scope of immunity that courts have

reach a broad audience by amplifying the biggest sellers—disinformation fraudsters, white supremacists, neo-Nazis, and other fanatics—and drowning out the voices of ordinary people.[45]

The revised immunity under the Big Tech Accountability Act, by contrast, would discourage this kind of amplification by holding platforms that do it accountable, while leaving fully protected those platforms that provide an open, un-curated platform, giving a fighting chance for ordinary people to be heard above the rage of the racists and propagators of disinformation. The Big Tech Accountability Act would amend the Communications Decency Act to remove immunity only for internet companies that (a) target the dissemination of the content to an individual or specific group of individuals; (b) act knowingly, recklessly, or negligently in encouraging or facilitating the spread of disinformation or violence; or (c) intentionally engage in a course of business that receives a financial benefit from amplifying disinformation or violence. And it would create new liability for internet companies only when they engage in this type of harmful amplification of fraudulent disinformation or violence.

C. *Existing Laws Are Inadequate to Address the Threat Posed by Big Tech*

Some have argued that existing laws, such as fraud, defamation, and perjury laws, under which persons making certain harmful false statements (on or off the internet) can already be held accountable, are as far as the law should go to address disinformation and violence promotion on the internet.[46] But the dangers of disinformation and violence on the internet do not primarily flow from the making of false or violent statements by individual people. Rather, they are the result of systematic selecting, amplifying, and targeting by powerful corporations of fraudulent and violent statements—a process that magnifies the destructive power of a false or violent statement to a historically unprecedented level. Current law provides no remedy for this conduct and this harm. To the contrary, through § 230 of the Communications

applied under § 230 and arguing that this expansive interpretation is unsupported by the text or intent of the statute); *see also supra* note 23.

45. In one chilling example, in February 2019—a year before the arrival of COVID-19 and almost two years before the availability of COVID-19 vaccines—it was reported that non-profit organizations attempting to post public service announcements promoting vaccinations had to give up because YouTube's algorithms would redirect users from the pro-vaccine videos to baseless antivaccination propaganda videos. Brandy Zadrozny, *Drowned Out by the Algorithm: Vaccination Advocates Struggle to Be Heard Online*, NBC NEWS (Feb. 26, 2019, 2:26 PM), https://www.nbcnews.com/tech/tech-news/drowned-out-algorithm-pro-vaccination-advocates-struggle-be-heard-online-n976321 [https://perma.cc/KLP4-B7TM]; *see also supra* notes 2–9.

46. *See, e.g.*, Strossen, *supra* note 21.

Decency Act, current law thwarts any possible remedy.[47] The Big Tech Accountability Act would fix that.

D. *The Big Tech Accountability Act Would Reduce, Rather than Increase, the Ability of Powerful Politicians and Government Officials to Manipulate Social Media*

Some argue that enacting legislation to hold social media companies accountable will invite politically motivated enforcement by government officials. For example, if this enforcement mechanism had been available to the Donald Trump Justice Department, one could certainly imagine a Justice Department demand that social media companies take down any posting associated with Black Lives Matter or face enforcement action based on the dubious allegation that Black Lives Matter organizers were promoting unlawful violence at protests against police brutality. There are several reasons that this fear provides no basis to give Big Tech a pass on accountability.

First, nothing in the Big Tech Accountability Act would give the Department of Justice the power to impose a prior restraint on categories of speech based on the source of that speech. To the contrary, the Act provides for enforcement based only on specific unlawful solicitations of violence or specific conduct to knowingly make or amplify fraudulent civic disinformation.

Second, the Big Tech Accountability Act, like any other federal or state law, would be subject to all applicable constitutional constraints. An attempt by the Department of Justice to effectively shut down Black Lives Matter speech on social media would face compelling legal challenges on First Amendment, Equal Protection, and Due Process grounds.

Third, the risk of misuse of federal law enforcement powers by a corrupt Department of Justice to manipulate the substance of social media discourse is not unique to the Big Tech Accountability Act. While current law immunizes internet companies from being held liable as speakers or publishers of content on their platforms, these companies are subject to antitrust laws, criminal and civil fraud laws, securities laws, and many more—all of which could be misused by a corrupt Justice Department to manipulate content on social media.

Fourth, as with those other laws, government enforcement of the Big Tech Accountability Act would necessarily go through the courts and be subject to judicial review, providing a check against misuse.

Finally, the danger of government manipulation of social media companies for self-serving political purposes is arguably greater under our

47. Section 230 prohibits treating internet companies "as the publisher or speaker of any information provided by another" person or entity. 47 U.S.C. § 230(c)(1). While the Act states that it does not preempt any federal criminal law, *id.* § 230(e)(1), no such law directly addresses internet company amplification of disinformation and threats of violence.

current system in which the companies have immunity for their conduct in screening and amplifying content. Under current law, neither private parties, state governments, nor the federal government can hold social media companies legally accountable for promoting unlawful conduct.[48] But in this vacuum, powerful politicians and government officials are free to use their bully pulpit, the *threat* of regulation, or unrelated law enforcement actions, to manipulate how social media companies screen and target. Moving this oversight from the back room into the open and into the courts would ultimately reduce, rather than increase, the risk of corrupt government manipulation of social media companies.

E. *Nothing in the Big Tech Accountability Act Would Increase the Risk of Discrimination on Social Media Platforms*

In a similar vein, some claim that any attempt to hold Big Tech accountable for promoting disinformation and violence will backfire and encourage the big social media companies to discriminate against persons of color and civil rights organizations. This argument suffers from some of the same flaws as the notion that accountability for Big Tech will increase the risk of corrupt government manipulation of social media.

First, neither § 230 nor any other aspect about the current system protects persons of color and other marginalized groups from discrimination on the internet. To the contrary, online discrimination is one of the many problems with the current system. Indeed, one study suggested that social media companies are more likely to flag and screen content posted by black people than by white people.[49]

To suggest that discouraging social media companies from discriminating against racial groups requires permitting them to facilitate racist violence by white supremacists and neo-Nazis without accountability is backwards. This rationale is akin to suggesting that we should not penalize property owners who allow terrorists or racists to use their properties to facilitate violent attacks because holding them accountable might cause them to exclude persons of color from their properties. But we do not take that counterintuitive approach; instead, we have laws prohibiting racial discrimination in public accommodations. Similarly, the answer to racial discrimination by social media companies is not to leave them free to facilitate racist violence on their platforms, but instead to treat internet companies like public accommodations and

48. *See supra* note 47.

49. Shirin Ghaffary, *The Algorithms That Detect Hate Speech Online Are Biased Against Black People*, VOX: RECODE (Aug. 15, 2019, 11:00 AM), https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter [https://perma.cc/T7XW-FH7H].

prohibit racial discrimination by such companies.[50]

F. *The Claim that Regulation of Internet Platforms Would Strengthen the Biggest Social Media Companies at the Expense of Small Internet Companies Is Misguided and Misleading*

Another frequent objection to holding internet companies accountable is that accountability would hit hardest upon small businesses, who have fewer resources to comply and defend against litigation, and thereby only serve to strengthen the biggest offenders. This objection ignores the actual substance of the Big Tech Accountability Act and boils down to an unsustainable argument against government regulation of *any* business.

By creating new liability for social media companies that use algorithms or other sorting methods to amplify and target fraudulent civic disinformation and violence, the Big Tech Accountability Act is most clearly directed at companies that have adopted a business model of profiting from promoting unlawful material. The notion that this approach would more likely ensnare small companies trying to promote their lawful businesses on the internet, rather than the Big Tech companies whose biggest profit center lies in the promotion of unlawful material, makes no sense on its face.

Further, the argument that government regulation will harm small companies least able to afford compliance is a convenient shield against all government regulation of business. The same argument could be made against environmental regulation because the biggest most powerful polluters have the most resources to avoid or defend against the law; food safety laws, on the ground that they pose more challenging compliance issues for small restaurants and grocers than industrial food conglomerates; and worker protection laws, on the ground that small businesses have fewer resources and less flexibility to comply than global corporations. Similar arguments could be made with respect to any business regulation. It is no surprise then, that the most vociferous objectors to internet platform regulation are the big global technology companies.

G. *The Likelihood that Big Internet Companies Would Need to Change Their Business Models to Comply with the Big Tech Accountability Act Is Not an Argument Against the Act*

There is little doubt that complying with the Big Tech Accountability Act could require the largest internet companies to substantially change their business models. This is as it should be. The model of the major

50. Kristen Clarke & David Brody, *It's Time for an Online Civil Rights Act*, THE HILL (Aug. 3, 2018, 3:30 PM), https://thehill.com/opinion/civil-rights/400310-its-time-for-an-online-civil-rights-act?rl=1 [https://perma.cc/GD6F-GC3F].

internet companies has served their owners well, allowing a handful of people to achieve a level of personal wealth nearly unprecedented in human history. But a model that is based on collecting and exploiting *everyone's* personal information, on manipulating people's online experience, and on amplifying and promoting dangerous disinformation and violence to maximize profit does not deserve protection. It deserves regulation and reform.

CONCLUSION

All of the reforms set out in the Big Tech Accountability Act could be enacted in a manner consistent with the First Amendment and would build on existing time-tested models for holding people accountable for fraudulent and other criminal acts that are now being facilitated by social media companies. And the reforms are entirely consistent with the manner in which we have traditionally regulated corporations whose business practices threaten significant public harm. They would likely require the biggest social media companies to make significant reforms to their business model. But that is exactly what we need to happen if we want an internet that is compatible with a functioning democracy and rational self-government.

THE PROPOSED BIG TECH ACCOUNTABILITY ACT—FULL TEXT

THE BIG TECH ACCOUNTABILITY ACT

A Bill to foster accountability for digital content providers.

Section 1. Short Title.

This Act may be cited as the "Big Tech Accountability Act".

Section 2. Purpose.

> The purpose of this Act is to foster accountability by online platforms and other internet service providers; to protect internet users, voters, and the broader community from the dangers of rampant amplification of disinformation and violence; and to protect online personal privacy and autonomy against commercial exploitation.

Section 3. Liability for Promoting Fraudulent Civic Information.

(a) Chapter 47 of the United States Code Title 18 is amended by

adding at the end the following:

Section 1041. False Information About Essential Government Services or Processes.

(a) **In general**—Whoever, in interstate or foreign commerce, knowingly conveys or disseminates fraudulent civic misinformation, for the purpose or with the reasonable expectation of causing other persons to believe and rely or act upon such information in a manner reasonably expected to cause substantial public harm, shall be fined under this title or imprisoned not more than 5 years, or both.

(b) **Publishing Entity Liability.** Any publishing entity, or person acting on its behalf who, in interstate or foreign commerce, aids in the dissemination of fraudulent civic misinformation that violates subsection (b) of this section, by

(1) knowingly disseminating, publishing, or broadcasting fraudulent civic misinformation, or

(2) conducting individualized targeting to disseminate, publish, or broadcast the fraudulent civic misinformation, with reckless disregard for the risk of substantial public harm shall be fined under this title or imprisoned not more than 2 years, or both.

(c) **Limitations.** Nothing in this section shall be construed to prohibit, impair, or limit:

(1) efforts to report or correct false or misleading information;

(2) good faith efforts to summarize or explain facts pertaining to essential government services or processes or data, guidance, or other information conveyed by government agencies;

(3) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or political subdivision of a State, or of any intelligence agency of the United States; or

(4) expressions of opinion about, including disagreement with, facts pertaining to essential government services or processes or data, guidance, or other information conveyed by government agencies.

(d) **Definitions.**

(1) "Publishing entity" means any print publisher; radio-broadcast licensee; broadcast, cable, or local television station; provider of an interactive computer service as defined in 47 U.S.C. § 230(f)(2); covered online platform as defined in 47 U.S.C. § 232(d)(1); or agency or medium for the dissemination of advertising.

(2) "Fraudulent civic misinformation" means:

(A) Materially false, fraudulent, or misleading information pertaining to essential government services or processes, including government services concerning public health and safety, voting and voter registration, elections, the census, civil rights, and education; or

(B) Data, guidance, or information that is materially false, fraudulent, or misleading and that is falsely attributed to a government agency, or falsely asserted to have been sanctioned or authored by a government agency.

"Fraudulent civic misinformation" does not include any statement or information accompanied by a prominent disclaimer that clearly characterizes the statement or information as fiction, satire, humor, or criticism, if the disclaimer is presented in a way that is reasonable under the circumstances.

(3) "Individualized targeting" occurs when a publishing entity:

(A) performs or causes to perform any computational process (including one based on

algorithmic models, machine learning, statistical analysis, or other data processing or artificial intelligence techniques) designed to transmit or display, highlight, emphasize, or make more prominent, the content to a subset of the users of such platform selected based on personal information pertaining to the individuals who make up the subset of users; or

(B) allows another person to instruct a publishing entity to transmit or display, highlight, emphasize, or make more prominent, the content to a subset of the users of such publishing entity, including by providing to such person a list of individuals, contact information of individuals, or other personal information that can be used to identify individuals.

Provided, however, that displaying, highlighting, emphasizing, or making more prominent, content in direct response to requests made or search terms entered by an individual, such that any individual making such requests or entering such search terms would produce the same display, does not constitute individualized targeting under this section.

(4) "Personal information" means any information that is linked or reasonably linkable to a specific individual or a specific device, including but not limited to an individual's actual or perceived characteristics or demographics and information that may be derived from such individual's internet browsing history, and including de-identified information.

(5) "Substantial public harm" means direct and actual damage to property; grievous personal injury or death; damage to the health or safety of the general public; or diversion of law enforcement or other public health and safety authorities from their duties; or deterring, intimidating, or preventing persons from voting, exercising their civil rights, or answering questions in connection with any census or survey provided for by title 13 of the United

States Code.

Section 1042. Civil Penalties, Injunction, and Damages for Violations of Section 1041.

(a) **Civil Enforcement by the Attorney General.** The Attorney General may bring a civil action in the appropriate United States district court against any person who engages in conduct constituting an offense under subsection (b) or (c) of section 1041 and, upon proof of such conduct by a preponderance of the evidence, such person shall be subject to a civil penalty of not more than $50,000 for each violation or the amount of compensation which the person received or offered for the prohibited conduct, whichever amount is greater. The imposition of a civil penalty under this subsection does not preclude any other criminal or civil statutory, common law, or administrative remedy, which is available by law to the United States or any other person.

(b) **Injunctive Relief.** If the Attorney General has reason to believe that a person is engaged in conduct constituting an offense under subsection (b) or (c) of section 1041, the Attorney General may petition an appropriate United States district court for an order prohibiting that person from engaging in such conduct. The court may issue an order prohibiting that person from engaging in such conduct if the court finds that the conduct constitutes such an offense. The filing of a petition under this section does not preclude any other remedy which is available by law to the United States or any other person.

(c) **Civil Action for Damages.** Whoever engages in conduct constituting an offense under subsection (b) or subsection (c) of section 1041 is liable in a civil action to any person incurring expenses incident to any emergency or investigative response to the information that violated subsection (b) of section 1041; to any person incurring expenses incident to any efforts required to correct the fraudulent civic misinformation; to any person incurring injury, illness, or loss of life, loss of personal property, loss of an opportunity to vote in an election, loss of civil rights, loss or denial of government services, or expenses, including medical or legal expenses, as a result of the fraudulent civic misinformation; or for injunctive or other equitable relief to prevent substantial public harm. The court may grant any such relief upon finding by a preponderance of

the evidence that the defendant has engaged in conduct constituting an offense under subsection (b) or subsection (c) of section 1041.

Section 4. Liability for Promoting Encouragement of Violence.

(a) Chapter 21 of the United States Code Title 42 is amended by adding the following:

Section 1986a. Criminal Liability for Amplifying Encouragement of Violence.

(a) **In general**—Any person who knowingly and intentionally disseminates on the internet, in interstate commerce and in a manner calculated to reach 500 or more viewers, a communication that solicits, commands, induces, encourages, or otherwise endeavors to persuade another person or persons to kidnap or cause death or serious bodily injury to any person, or to engage in conduct constituting a felony that has as an element the use, attempted use, or threatened use of physical force against property or against the person of another, in violation of the laws of the United States, including but not limited to 42 U.S.C. § 1985 and 42 U.S.C. § 1986, whether or not such communications identify a specific person or property as the target of such actions, shall be fined under this title or imprisoned not more than 2 years, or both.

(b) **Publishing Entity Liability.** Any publishing entity or person acting on behalf of a publishing entity, who, in interstate or foreign commerce,

(1) disseminates, publishes, or broadcasts a communication that solicits, commands, induces, encourages, or otherwise endeavors to persuade another person or persons to kidnap or cause death or serious bodily injury to any person, or to engage in conduct constituting a felony that has as an element the use, attempted use, or threatened use of physical force against property or against the person of another, in violation of the laws of the United States, including but not limited to 42 U.S.C. § 1985 and 42 U.S.C. § 1986, whether or not such communications identify a specific person or

property as the target of such actions;

(2) conducts individualized targeting to disseminate, publish, or broadcast such communication; and

(3) causes the communication to be viewed, seen, or read 10,000 or more times within the United States by means of dissemination, publication, or broadcast that is controlled or owned, in whole or in part, by the publishing entity,

shall be fined under this title or imprisoned not more than 2 years, or both.

(c) **Definitions.**

(1) "Individualized targeting" occurs when a publishing entity:

(A) performs or causes to perform any computational process (including one based on algorithmic models, machine learning, statistical analysis, or other data processing or artificial intelligence techniques) designed to transmit or display, highlight, emphasize, or make more prominent, the content to a subset of the users of such platform selected based on personal information pertaining to the individuals who make up the subset of users; or

(B) allows another person to instruct a publishing entity to transmit or display, highlight, emphasize, or make more prominent, the content to a subset of the users of such publishing entity, including by providing to such person a list of individuals, contact information of individuals, or other personal information that can be used to identify individuals;

Provided, however, that displaying, highlighting, emphasizing, or making more prominent, content in direct response to requests made or search terms entered by an individual, such that any individual making such requests or entering such search terms would produce the

same display, does not constitute individualized targeting under this section.

(2) "Personal information" means any information that is linked or reasonably linkable to a specific individual or a specific device, including but not limited to an individual's actual or perceived characteristics or demographics and information that may be derived from such individual's internet browsing history, and including de-identified information.

(3) "Publishing entity" means any print publisher; radio-broadcast licensee; broadcast, cable, or local television station; provider of an interactive computer service as defined in 47 U.S.C. § 230(f)(2); covered online platform as defined in 47 U.S.C. § 232(d)(1); or agency or medium for the dissemination of advertising.

Section 1986b. Civil Penalties, Injunction, and Damages for Violations of Section 1986a.

(a) **Civil Enforcement by the Attorney General.** The Attorney General may bring a civil action in the appropriate United States district court against any person who engages in conduct constituting an offense under section 1986a and, upon proof of such conduct by a preponderance of the evidence, such person shall be subject to a civil penalty of not more than $50,000 for each violation or the amount of compensation which the person received or offered for the prohibited conduct, whichever amount is greater. The imposition of a civil penalty under this subsection does not preclude any other criminal or civil statutory, common law, or administrative remedy which is available by law to the United States or any other person.

(b) **Injunctive Relief.** If the Attorney General has reason to believe that a person is engaged in conduct constituting an offense under section 1986a, the Attorney General may petition an appropriate United States district court for an order prohibiting that person from engaging in such conduct. The court may issue an order prohibiting that person from engaging in such conduct if the court

finds that the conduct constitutes such an offense. The filing of a petition under this section does not preclude any other remedy which is available by law to the United States or any other person.

(c) **Civil Action for Damages.** Whoever engages in conduct constituting an offense under section 1986a is liable in a civil action to any person, group of persons, or entity against whom such communication were made, who were injured or harmed as a consequence of such communication, or whose property was injured or harmed as a consequence of such communication, whether or not such person or entity was identified by name in the communication, in an action for damages occasioned by such communication, for injunctive relief, or for other appropriate relief. The court may grant any such relief upon finding by a preponderance of the evidence that the defendant has engaged in conduct constituting an offense under section 1986a.

Section 5. Amendments to Section 230 and Restrictions on Targeted Advertising and Collection and Sale of Personal Information.

(a) Section 230(c)(1) of the Communication Act of 1934 (47 U.S.C. 230(c)(1)) is amended to read:

(1) **Treatment of Publisher or Speaker.**

~~No 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~~.

In any civil action against a provider or user of an interactive computer service ("ICS") arising from information provided by another information content provider, the ICS shall not be held liable as the publisher or speaker of that information unless the ICS:

1. Engages in targeting the dissemination of the content to an individual or specific group of individuals;

2. Acts knowingly, recklessly or negligently in encouraging or facilitating the spread of misinformation, disinformation, or violence; or

3. Intentionally engages in a course of business that receives a financial benefit from amplifying misinformation, disinformation, or violence.

(b) Section 230(f) of the Communication Act of 1934 (47 U.S.C. 230(f)) is amended by adding the following:

(5) **Targeting the Dissemination of Content.**

An ICS engages in "targeting the dissemination of content to a particular individual or specific group of individuals" if the ICS, or an agent, affiliate, vendor, or other person acting on behalf of such ICS—

(A) performs or causes to perform any computational process (including one based on algorithmic models, machine learning, statistical analysis, or other data processing or artificial intelligence techniques) designed to transmit or display, highlight, emphasize, or make more prominent, the content to a subset of the users of such platform selected based on personal information pertaining to the individuals who make up the subset of users; or

(B) allows another person to instruct an ICS to transmit or display, highlight, emphasize, or make more prominent, the content to a subset of the users of such ICS, including by providing to such ICS a list of individuals, contact information of individuals, or other personal information that can be used to identify individuals.

Provided, however, that displaying, highlighting, emphasizing, or making more prominent, content in direct response to requests made or search terms entered by an individual, such that any individual making such requests or entering such search terms would produce the same display, does not constitute targeting under this section.

(6) **Personal Information.**

The term "personal information" means any information that is linked or reasonably linkable to a specific individual or a

specific device, including but not limited to an individual's actual or perceived characteristics or demographics and information that may be derived from such individual's internet browsing history, and including de-identified information.

(c) Chapter 5 of Title 47, United States is amended by adding the following:

Section 232. Restrictions on Targeted Online Advertising

(a) **Restrictions on Advertisements Targeted at Individuals or at Specific Groups of Individuals.**

(1) Restrictions. A covered online platform or an agent, affiliate, vendor, or other person acting on behalf of such a platform, may not target the dissemination of an advertisement on such platform to an individual or to a specific group of individuals on any basis.

(2) Actions Constituting Targeting. A covered online platform or an agent, affiliate, vendor, or other person acting on behalf of such a platform shall be considered to target the dissemination of an advertisement to an individual or to a specific group of individuals if such platform—

(A) (i) performs or causes to perform any computational process (including one based on algorithmic models, machine learning, statistical analysis, or other data processing or artificial intelligence techniques) designed to transmit or display, highlight, emphasize, or make more prominent, the advertisement to a subset of the users of such platform selected based on personal information pertaining to the individuals who make up the subset of users; or

(ii) allows another person to instruct a covered online platform to transmit or display, highlight, emphasize, or make

more prominent, the advertisement to a subset of the users of such platform, including by providing to such platform a list of individuals, contact information of individuals, or other personal information that can be used to identify individuals; and

(B) receives a fee or other payment, directly or indirectly, for disseminating the advertisement or providing the information.

(3) Exception: Targeting Individuals within a Governmental District. Subsection (a) does not apply to the targeting of the dissemination of an advertisement to an individual residing in, or to a device located in, a Governmental District.

(4) Sorting Based on Individual Search Terms or Requests. Displaying, highlighting, emphasizing or making more prominent, advertising or other content in direct response to requests made or search terms entered by an individual, such that any individual making such requests or entering such search terms would produce the same display, does not constitute targeting under subsection (a).

(b) **Private Right of Action.**

(1) Enforcement by Individuals.

(A) In general. Any person alleging a violation of this section by a covered online platform may bring a civil action in any court of competent jurisdiction, State or Federal.

(B) Relief. In a civil action brought under this paragraph in which the plaintiff prevails, the court may award—

(i) an amount not less than $100 and not greater than $1,000 per violation

against any person who negligently violates a provision of this section;

(ii) an amount not less than $500 and not greater than $5,000 per violation against any person who recklessly, willfully, or intentionally violates a provision of this section;

(iii) reasonable attorney's fees and litigation costs; and

(iv) any other relief, including equitable or declaratory relief, that the court determines appropriate.

(C) Injury in Fact. A violation of this section constitutes a concrete and particularized injury in fact to an individual.

(2) Invalidity of Pre-Dispute Arbitration Agreements and Pre-Dispute Joint Action Waivers.

(A) In general. Notwithstanding any other provision of law, no pre-dispute arbitration agreement or pre-dispute joint action waiver shall be valid or enforceable with respect to a dispute arising under this section.

(B) Applicability. Any determination as to whether or how this subsection applies to any dispute shall be made by a court, rather than an arbitrator, without regard to whether such agreement purports to delegate such determination to an arbitrator.

(C) Definitions. In this subsection:

(i) "Pre-Dispute Arbitration Agreement" means any agreement to arbitrate a dispute that has not arisen at the time of making the agreement.

(ii) "Pre-Dispute Joint-Action Waiver" means an agreement, whether or not part of a pre-dispute arbitration agreement, that would prohibit, or waive the right of, one of the parties to the agreement to participate in a joint, class, or collective action in a judicial, arbitral, administration, or other forum, concerning a dispute that has not yet arisen at the time of making the agreement.

(iii) "Dispute" means any claim related to an alleged violation of this section and between an individual and a covered organization.

(c) **Enforcement by Attorney General.**

(1) Civil Action for Fines. The Attorney General may bring a civil action in the appropriate United States district court against any person who engages in conduct in violation of this section. In any such action the district court may award appropriate relief in including a civil penalty of not more than $50,000 for each violation or the amount of compensation which the person received or offered for the prohibited conduct, whichever amount is greater. The imposition of a civil penalty under this subsection does not preclude any other remedy which is available by law to the United States or any other person.

(2) Injunctive Relief. If the Attorney General has reason to believe that a person is engaged in conduct in violation of this section, the Attorney General may petition an appropriate United States district court for an order prohibiting that person from engaging in such conduct. The court may issue an order prohibiting that person from engaging in such conduct if the court finds that the conduct constitutes such a violation. The filing of a

petition under this section does not preclude any other remedy which is available by law to the United States or any other person.

(d) **Effective Date.** Section 232 of Title 47, United States Code shall take effect 3 months after the date of the enactment of this Act.

(e) **Definitions.** In this section:

(1) "Covered Online Platform" means any website, web application, mobile application, smart device application, digital application (including a social network, or search engine), or advertising network (including a network disseminating advertisements on another website, web application, mobile application, smart device application, or digital application).

(2) "Personal Information" means any information that is linked or reasonably linkable to a specific individual or a specific device, including but not limited to an individual's actual or perceived characteristics or demographics and information that may be derived from such individual's internet browsing history, and including de-identified information.

(3) "Governmental District" means any of the following:

(A) Each State, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and the United States Virgin Islands.

(B) Indian and tribal lands as defined and recognized under federal law.

(C) A county, municipality, city, town, township, village, borough, or similar unit of general government incorporated under

State law or as defined by the Census Bureau; or

(D) A congressional district.

Section 233. Restrictions on Collection, Aggregation, and Sale of Personal Information

(a) **Congressional Finding.**

The Congress finds that the widespread practice of websites, internet service companies, and data brokers, among others, collecting, aggregating, and selling personal information of individuals derived from their internet activity ("online personal information") poses a grave threat to personal privacy and autonomy.

(b) **Congressional Purpose and Policy.**

The Congress declares it to be its purpose and policy to protect personal privacy and autonomy by restricting the exploitive collection, aggregation, and sale of online personal information and to prohibit the collection, aggregation, and sale of any individual's online personal information without the genuine, informed and meaningful consent of such individual.

(c) **FTC Recommendations to Prohibit the Aggregation and Sale of Personal Information without Consent.**

In order to protect personal privacy and autonomy, the Federal Trade Commission is hereby directed to study and make recommendations for specific reforms and legislation restricting the collection, aggregation, or sale of online personal information and prohibiting the collection, aggregation, or sale of any individual's online personal information without the genuine, informed, and meaningful consent of such individual. Among other provisions, the FTC shall include in its recommendations, provisions establishing that blanket consent obtained as a condition to accessing information or services on the internet shall not be considered meaningful consent.

(d) **Deadline for FTC Recommendations.**

> The Federal Trade Commission shall submit a report to Congress containing the recommendations required by this section within 120 days of enactment of this Act.