

STATEMENT FOR THE RECORD BY DONALD K. SHERMAN,
VICE PRESIDENT AND CHIEF COUNSEL,
CITIZENS FOR RESPONSIBILITY AND ETHICS IN WASHINGTON (CREW)

SUBMITTED TO THE HOUSE COMMITTEE ON ENERGY AND COMMERCE
HEARING ON
“HOLDING BIG TECH ACCOUNTABLE: LEGISLATION TO BUILD A SAFER
INTERNET”

DECEMBER 9, 2020

Chairman Pallone, Ranking Member McMorris Rodgers, and members of the Committee, thank you for the opportunity to submit this statement for the record on legislation moving through Congress to hold Big Tech accountable to build a safer internet.

Technology, including the advancement of social media platforms, has had a tremendous impact on access to democracy. However, the lack of sufficient government oversight or self-regulation has allowed bad actors to use these platforms to undermine democratic institutions in the United States and other countries. For example, CREW [documented](#) Twitter’s [failure](#) to police Kellyanne Conway’s abuse of the platform to violate the Hatch Act more than 50 times despite the company’s Terms of Service and rules requiring users to use the platform in compliance with all applicable laws. These vulnerabilities were laid bare during the last year as extremism and misinformation were allowed to proliferate on social media and former President Trump and others used Big Tech assets and platforms to foment discord that eventually led to an armed insurrection of the United States Capitol. Despite [numerous](#) prior [warnings](#) about the [former](#) president’s abuse of social media [platforms](#) in violation of their own policies--including by promoting misinformation and violence-- Facebook, Twitter, and other companies [only](#) took [action](#) to de-platform Trump after he incited the violent riot on January 6, 2021.

I write on behalf of my organization, Citizens for Responsibility and Ethics in Washington (CREW), today to underscore the need for prompt and thorough action. CREW is a non-partisan, non-profit organization committed to ensuring the integrity of our democratic institutions, combating the impact of monied special interests on our political system, and promoting ethical governance.

As Congress considers policy changes to prevent these ongoing threats to our democratic institutions, and the Biden-Harris administration convenes an international Summit for Democracy, investigation of and accountability for Big Tech’s role in undermining democracy must be a priority. It is also critical that Congress push these platforms to take an active role in

repairing the standards and institutions that they have helped erode. Today's hearing and the legislation under consideration by the Committee are powerful tools to advance these goals. Indeed, the time for reform is past due. Big Tech has had numerous opportunities to self-regulate and to improve its oversight of online harassment, misinformation and other abusive practices that threaten our democracy. The government must intervene by stepping-up its regulation and enforcement efforts to prevent abuses of the horrific events of January 6th from ever happening again.

Additional Reforms are Needed to Curb the Destabilizing Nature of Extremism, Harassment and Misinformation

The failure of the federal government or industry to effectively regulate Big Tech presents an ongoing threat to our democracy. While some of these challenges are well documented, two stand out. First, tech companies have failed to curb the proliferation of misinformation, especially non-English language content, shared on social media platforms. Secondly, online extremism, hate, and harassment, especially directed at women, girls, and members of other historically marginalized communities continues to pose significant threats. That's one reason why, ahead of today's Democracy Summit, the Biden-Harris administration [included](#) the advancement of gender equity, racial justice and LGBTQI+ equality as key parts of its plan to bolster American democracy.

Social media networks' failure to appropriately address misinformation in languages other than English provides a glaring example of why Congressional intervention is urgent. For instance, in April 2021, one study [found](#) that Facebook flags only 29% of misinformation in Spanish, as compared to 70% of comparable material in English. According to [reporting](#) by *Prism*, many social media sites popular with Asian Americans, such as the Chinese-language social media app, WeChat, have misinformation problems that largely go unchallenged or with less moderation than posts in English. A November 2021 [report](#) noted that even though YouTube banned the Alex Jones site InfoWars, it ignored the "[Vietnamese-American version of Alex Jones](#)" for months—only taking action after a segment about the subject aired on John Oliver's *Last Week Tonight*. Research by Equis Research and Equis Labs found that as of [October 2021](#), Facebook still had Spanish-language posts active from November 2020 that promoted [election misinformation](#) without any warning labels and that QAnon content banned in English "[continued to spread](#) in Spanish."

Failure to take sufficient action threatens both public safety and our democratic institutions. Reports indicate that [dark money funded](#) disinformation campaigns targeted [immigrants and communities of color](#) to suppress their turnout in the 2020 election. This year, the Latinx community was flooded with disinformation [about the COVID-19](#) vaccine. These efforts highlight the dangerous nexus between unaccountable money in politics and racism, and how

they intersect to exploit the lack of federal enforcement and self-regulation over social media. Several [Members of Congress](#), including some on this Committee, have demonstrated leadership on potential reforms by [urging](#) Big Tech CEOs to combat non-English language disinformation, and by introducing [legislation](#) that would create an exception under Section 230 of the Communications Decency Act for platforms that have algorithms that promote health misinformation related to an existing public health emergency.

The [international](#) human rights [community](#) has long [recognized](#) that gender equity and the empowerment of women are essential to a functioning democracy. As the Carnegie Endowment for International Peace [noted](#), “Democracy is as much about citizenship rights, participation and inclusion as it is about political parties, elections, and checks and balances. The quality of democracy is determined not only by the form of institutions, but also by the extent that different social groups participate in these institutions.”

Social media has been [integral](#) to providing women and girls greater access to political participation. However, visceral and public hate on social media can lead to women and girls censoring themselves, thus silencing voices that are critical elements of a functioning democracy. According to one international [survey](#), approximately one in four women in the United States and seven other countries reported experiencing online abuse or harassment. Even more disturbing, more than 40 percent of the women said the online attacks led them to fear for their physical safety, while more than 50 percent reported trouble sleeping, loss of self-esteem and panic attacks. In fact, a 2015 [United Nations](#) report [found](#) that “cyber violence” including online abuse and harassment can be as damaging to women and girls as physical violence.

Gendered attacks impact women across sectors, but particularly in [journalism](#) and government. Online harassment is leading many female [journalists](#) to leave the field. Another study by [She Persisted](#) found that online attacks against women in politics are “overwhelmingly more personal and negative,” and “often refer to their gender identity and value as women - as opposed to their policy proposals and ideas, as is the case for male politicians.”

Unsurprisingly, online abuse also has an intersectional impact. According to a [2020 study](#) conducted by the Institute for Strategic Dialogue, researchers found that women and people of color were “far more likely than men to be abused on Twitter.” Another study concluded that [women of color](#) face “exponentially” more online harassment. Amnesty International [found](#) that women of color were 34% more likely to encounter harassment than their white counterparts, and that Black women were “disproportionately targeted” including being “84% more likely than white women to be mentioned in abusive or problematic tweets.” Earlier this year, an [Anti-Defamation League](#) study reported that 64% of LGBTQ+ respondents have been harassed online, and at a disproportionately higher rate than other identity groups. The study also found that LGBTQ+ respondents were more likely to suffer severe forms of harassment, including

electronic distribution of humiliating photos, dissemination of false or private information, stalking, and physical threats.

Research by *She Persisted* [revealed](#) that social media platforms were “fertile ground for the spread of gendered disinformation, to be understood as the spread of deceptive or inaccurate information and images against women political leaders, journalists and female public figures.” Online abuse, harassment and disinformation have been tied to violence against, and mental health challenges suffered by, women, people of color, and people in the LGBTQI+ community. The failure of social media companies to effectively monitor, mitigate, and police online harassment has dissuaded many women in the [United States](#) and [across the globe](#) from pursuing careers in government service, a trend with far-reaching consequences.

Following the insurrection at the United States Capitol, this Committee held a hearing to examine the role played by Big Tech’s failure to provide sufficient oversight of their platforms. These companies and their products have been exploited to support white supremacy and the violent extremism on display on January 6, 2021 and many other incidents. Predictably, when the Chief Executive Officers of Facebook, Twitter and Google appeared before this Committee in March 2021, the executives acknowledged that their companies continued to struggle with curbing misinformation and [suggested](#) that significant and ongoing reforms by Big Tech and the federal government were necessary to address these abuses.

Sundar Pichai of [Google](#) testified, “Our work is never done, and we continue to learn and improve from one election cycle to the next, and continue to evolve our policies.” Mark Zuckerberg of [Facebook](#) said, “misinformation is an ongoing challenge for us. With millions of Americans using our services every day, there will always be things we miss.” Jack Dorsey of [Twitter](#) testified, “Every day Twitter grapples with complex considerations on how to address extremism and misinformation. How do we prevent harm, while also safeguarding free expression and the right of diverse individuals to express a range of views?”

It is important to acknowledge that leading up to, and in the aftermath of, the 2020 election, these companies took some steps to remove misinformation from their platforms, curb abuse, and develop new policies to address extremism and civil rights abuses. But there is more work for industry and policymakers to do. Members of Congress have a responsibility to investigate whether tech platforms are making inroads on promises to combat misinformation, especially when progress reports are often choreographed to the pace of Congressional hearings.

The Proposed Legislation Will Help Ensure Oversight and Accountability for Big Tech

The bills under consideration by the Committee propose significant reforms that will help to advance accountability for Big Tech companies who do not effectively prevent their platforms

from being used to engage in civil rights violations, misinformation, and harassment and abuse. As Chairman Pallone has described, H.R. 3421, the “Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act,” would reform Section 230 to help address the proliferation of misinformation by (1) replacing immunity under (c)(1) for third party “information” with immunity for third-party “speech”; (2) removing Section 230 protections for paid advertisements; (3) prohibiting interactive computer service from pleading immunity under Section 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. H.R. 3451, the “Social Media DATA Act,” would require the Federal Trade Commission (FTC) to issue regulations that require large digital advertising platforms to maintain and grant academic researchers and the FTC access to ad libraries that contain specific data on advertisements in a searchable, machine-readable format.

In order to address some of the civil rights concerns raised by users and activists, H.R. 3611, the “Algorithmic Justice and Online Platform Transparency Act” would prohibit the use of algorithmic processes that discriminate based on race, age, gender, ability, and other protected characteristics. The bill also promotes transparency and oversight by requiring platforms to describe to users the types of algorithmic processes they use and to maintain detailed records describing these processes for review by the FTC-- in addition to creating an inter-agency task force to examine discriminatory algorithmic processes. Finally, H.R. 5439, the “KIDS Act,” would create new protections for online users under the age of 16 by prohibiting the amplification of harmful content to children and requiring websites to create mechanisms for users to report instances of harmful content. None of these proposed bills is a panacea and each will surely get further refined and improved through the legislative process, but they represent the Committee’s commitment to bring needed reform and accountability for the Big Tech industry. That alone is a positive development for public safety and democracy.

Conclusion

For years, civil rights and good government advocates have called on the federal government to take more aggressive action to regulate social media companies in order to facilitate better oversight of the threats that misinformation and online harassment, abuse, and extremism pose to our democracy. Lies and misinformation spread throughout social media exponentially faster than the truth. Following the carnage enabled by Donald Trump and his supporters, the Committee’s charge is even more pressing. We look forward to working with the Committee to develop legislative remedies to address these and other challenges to democratic institutions at home and abroad.