AMB. MARC C GINSBERG
PRESIDENT
COALITION FOR A SAFER WEB

TESTIMONY BEFORE
THE HOUSE ENERGY & COMMERCE SUBCOMMITTEE
ON CONSUMER PROTECTION & COMMERCE

SEPTEMBER 24, 2020

On behalf of the Coalition for a Safer Web (CSW) (www.coalitionsw.org) I am honored to appear before this timely and important Subcommittee hearing.

I request that my written testimony along with its attachments be entered into the record.

The American people confront a grave and present danger from the torrent of violent extremist incitement on social media platforms.

A toxic brew of extremist groups from the fringes of the political spectrum are hijacking and weaponizing the web to incite violence like never before – aided by technological infirmities of mainstream social media companies, the capacity of extremist groups to evade feeble firewalls, and the prevalence of web-based community boards such as 4chan, 8kun, and GAB which provide an unregulated safe haven for individuals and groups to recruit, plot, incite, and execute acts of domestic terror.

It is by no accident that the FBI now considers domestic extremist groups a first line threat to our safety on par with foreign terrorist organizations, such as ISIS and Al Qaeda.

Moreover, as I will explain in my testimony the mobile application known as TELEGRAM has become a global sanctuary from which extremist groups can actually plot and direct attacks in real time, as CSW discovered in its investigation of TELEGRAM accounts during the Portland riots.

The American people and their representatives in Congress confront a cosmic challenge which defies easy solution.

Major social media companies have taken it upon themselves to self-censor content based on widely divergent policies while failing in the most fundamental way to adequately protect their customers or Americans, writ large from the threats posed by extremists and their efforts to radicalize raw recruits to their various causes.

While major social media companies insist they are not publishers in order to avoid the penalties for being deemed so under Section 230 of the Communications Decency Act

(CDA) they are devoting more and more time to deciding (when Congress has not done it for them) which content may be uploaded, which content must be de-platformed, which falls in between, and, well, making it up each day depending how the prevailing political winds are blowing. CSW asserts, despite protests to the contrary by their executives and free speech advocates, that social media companies have become de facto publishers by taking the editor's road they have embarked upon to subjectively decide all manner of content visibility or invisibility.

To assert they remain innocent bystanders as extremist dis and misinformation land on their platforms is simply incorrect. But when it suits their purpose social media executives remain adamant that they are not liable for the witch's brew they purvey to the public. And we know why. Because the law is on their side, and not on the side of the public interest.

It is no way to run a railroad because we the passengers are the victims.

Because the business model of mainstream social media is totally dependent on ad revenue, there is no financial or legal incentive for Facebook, Twitter, YouTube, or Instagram to submit to independent oversight and accountability. They assert a mere moral obligation to engage in wishy washy content moderation. They cling to Section 230 as the Holy Grail, with good reason, because you and I know that without Section 230's content immunity their financial models would be subject to attack for failing to protect their customers from harm.

Meanwhile, extremist groups have devised ingenious work arounds to evade accountability, assisted by extremist-supporting web communications and hosting channels, benefiting from a deluge of disinformation and misinformation detrimental to our democracy.

CSW BACKGROUND

The Coalition for a Safer Web is a not-for-profit non-partisan organization under Section 501(c)(3) of the IRS Code formed in 2019 with six mission goals:

1. **Identify and advocate de-platforming of domestic and foreign social media extremist and hate incitement.**
2. **Advocate the de-platforming of the illicit sale of illegal substances.**
3. **Develop policy proposals to remedy the growing threat of fringe websites serving as "feeders" to super spread neo-Nazi, white nationalist incitement.**
4. **Pending Congressional action on Section 230 of the Communications Decency Act, promote creation of a new Social Media Standards Board.**
5. **Recommend new policy and technological software which would better enable major social media companies to interdict and permanently de-platform incitement of extremist violence and acts of terrorism.**
6. **Interdict the usage of web-based social media platforms by ISIS and other radical Islamic terrorist organizations.**

As a relatively new non-profit with a small staff, we like to describe our work as uncovering the proverbial needles in extremist haystacks -- or in this case we prefer a battlefield classification as "internet snipers" – taking out of action extremist inciters and their content incitement .

Since our inception our work has been cited in many major media outlets for its work:

- **Fake Covid Remedies: Uncovered criminal efforts by neo-Nazi/white nationalist groups to market illegal Covid remedies and branded neo-Nazi products to fund trans-national white nationalist groups.**
- **Christchurch Massacre Videos: Identified and exposed the failure of Facebook and Instagram to fulfill its pledge to irrevocably remove livestreamed videos of the Christchurch mosque massacre**
- **Black Hebrew Israelites: Exposed the use by Black Hebrew Israelites of fake Facebook, Instgram, and Twitter accounts, including stealing the identities of American rabbis.**
- **Sale of Illegal Substances: Exposed how Facebook, Instagram, and YouTube accounts are being used to sell illegal steroids and opioids.**
- **The "Plandemic Video: Exposed the role of the fake "Plandemic" video to spread anti-Semitism.**
- **QAnon: Uncovered QAnon's command & control digital distribution system and the contagion of QAnon accounts by neo-Nazi groups based in Germany and Russia.**
- **The "Base": Recommended to Congress additional economic sanctions on Russia for providing safe havens for far-right neo-Nazi groups and leaders, including Rinaldo Navarro, the leader of the notorious "accelerationist" neo-Nazi group known as "The Base."**

MAJOR SOCIAL MEDIA PLATFORMS ARE FAILING TO PROTECT THE AMERICAN PEOPLE

Congress has devoted considerable time and effort in recent years to determine why social media companies are failing to fulfill their public pledges to clean up their platforms from the scourge of extremist incitement. Both the House and Senate have demanded more accountability from the executives of major social media companies, each of whom have promised, pledged, assured, and reassured they are doing better to monitor and interdict extremist incitement.

Unfortunately, they have left a trail of broken promises, and the results are self-evident in representative examples I cite below:

■ ***YOUTUBE***

Unfortunately, YouTube's management has largely evaded public scrutiny accorded the executives of Facebook, Instagram, Twitter, and Google (despite Google being the

corporate parent of YouTube). All too often, when called to testify before Congress, representatives of its parent, Google/Alphabet have served as witnesses. Rarely have we seen a witness from YouTube be subjected to the type of examination we believe is merited given the blatant indifference and resistance set up by its senior management to de-platform the most obvious of toxic content.

Here are three examples of YouTube content which remains on its site despite numerous demands to de-platform it by many concerned citizens groups and web watchdog organizations:

- **YouTube's management has been stonewalling the Congress and the media on its failure to remove the 2015 murder video of WDBJ TV Virginia reporter Alison Parker. CSW has been serving as the intermediary between Senate Judiciary Committee and YouTube on behalf of the Parker family, to no avail.**

- **YouTube's management has ignored repeated demands that it remove thousands of videos showing prospective terrorists how to make a home-grown bomb – videos the FBI has corroborated were used by domestic terrorists to develop pipe bombs, including the bombs used at the Boston Marathon bombing in 2015 and the pipe-bomb found in the knapsack of Nikolas Cruz who committed the shooting at the Marjorie Stoneman Douglas HS in Parkland, FL in 2018.**

  I fail to comprehend how having these "how to make a pipe bomb videos available for years on YouTube can be brushed off as in the public interest by YouTube's management. Ms. Wojcicki and her staff deserve to be held accountable as accessories.

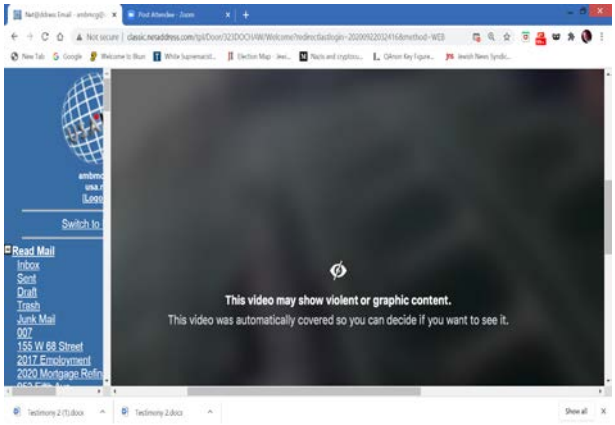
- **YouTube continues to provide a platform for neo-Nazi white nationalist extremist groups to incite and inspire recruiting. We have repeatedly written to YouTube's CEO Susan Wojcicki demanding that YouTube de-platform video games of Nazi-uniformed soldiers killing soldiers wearing Yellow Stars of David which represents digital shark bait for white nationalist recruiting operations since the videos are amplified across social media platforms to individual accounts, including TikTok.**

■ ***FACEBOOK***

CSW continues to uncover extremist content on Facebook and its affiliate, Instagram, which Facebook's executives assured the public has been permanently removed. While CSW acknowledges that Facebook's army of content moderators and its technological improvements have made significant inroads combatting extremist incitement, it continues to fail the most basic of its public pledges to keep content off its platform which it promised would never reappear again.

This reflects the paradox Congress confronts with respect to Facebook. And it is a paradox that is regrettably repeated over and over again.

Case in point – the Christchurch massacre live-streamed videos continue to reappear on Facebook and Instagram. Of the 15 Christchurch massacre videos we located on Facebook and Instagram since January, 2020, 13 remain. On some Facebook's artificial intelligence flagged them as graphic violence: "this video may show violent or graphic content, this video is automatically covered so you can decide if you want to see it…" A half-measure at best, a charade at worst. Providing an "R" rating does not stop a video which was never supposed to be on Facebook from being viewed.



CSW has been regularly communications with Facebook/s CEO – Sheryl Sandberg -- advising Facebook that we continue to uncover video streams of the massacre as well as suicide videos, and the 2015 video of slain journalist Alison Parker -- just like on YouTube it is available on Facebook posted by accounts in Arabic and other languages.

What this says to us is Facebook's vaunted artificial intelligence (AI) is simply unable to detect the reappearance of accounts with adverse content in foreign languages, or in the few instances it does – it leaves it to the viewer's discretion to review it. We even have uncovered neo-Nazi white nationalist accounts on Facebook Groups which resort to Yiddish words to camouflage white nationalist communications.

We are convinced that a primary cause of Facebook's inability to permanently de-platform content it pledged to do so is because of its over reliance on (AI) when it should incorporate digitally-sophisticated machine learning to provide direction to its AI – no different than a GPS navigation system directing drivers to their destination.

As our Senior Vice President for Content Moderation, Eric Feinberg, stated numerous times to major media outlets since the Christchurch massacre in March 2019, Facebook's AI is not trained nor can it adapt to real time/real world events by relying on AI alone. Mr. Feinberg developed a software technology based on real time human knowledge to train AI to locate such content, which he offered to make available to Facebook several years ago but was rebuffed. It is this software which enables CSW to identify content that Facebook's thousands of engineers and AI continue to miss.

Why won't Facebook and other social media platforms avail themselves of this type of helpful technology?

There are two reasons.

First, Facebook and other major platforms assert that innovative software would compel them to reveal their API (application programming index) – the crown jewels of their algorithm infrastructure -- the equivalent of software Cliff Notes.

To the best of our knowledge, Facebook's executives refuse to acquire any software which requires it to provide access to its API even under the most stringent of non-disclosure agreements.

Second, Section 230's content immunity provides a disincentive for social media companies to integrate and adopt better software to expedite and permanently de-platform extremist content. Candidly, CSW has been advised by counsel to several social media platforms that their legal departments fear that acquiring software from third parties may vitiate their Section 230 immunity from courts which would deem them assuming responsibility for the content they upload.

As this Subcommittee has heard via prior testimony, the business model of major social media companies is dependent on the amplification of viewer content – the more eyeballs/the more ad revenue. There is simply no financial incentive for Facebook or other advertising revenue-based platforms to ramp up their de-platforming software, and there is no legal consequence under Section 230 of the CDA for their failure to violate their de-platforming pledges.

■ THE ROLE OF ENCRYPTED APPLICATIONS IN RADICALIZATION

I would like to now turn to the role encrypted applications play in radicalization which enables trans-national fringe extremist and terrorist groups to operate below the radar.

The TELEGRAM Mobile Phone Application – A Super Spreader of Extremist Incitement

As they have been booted off mainstream social media platforms, extremist groups have prowled throughout the web to find more hospitable internet terrain from which to operate and incite acts of violence.

One portal which has been particularly hospitable to extremists is the mobile application known as TELEGRAM.

Created in 2013. TELEGRAM is a globally popular cloud-based chat and group messaging encrypted-enabled application promising its users protection from the prying eyes of intelligence agents and law enforcement.

Based in Dubai, United Arab Emirates, TELEGRAM's Russian-born founder Pavel Durov and his management team boast 200 million global users with over 220,000 separate TELEGRAM channels – most of which are innocent (e.g. artists, bakers, journalists, etc.).

But there are thousands of extremist channel accounts which incite and inspire violence and promote racial and religious bigotry – even when they issue absurd "disclaimers." On the radical fringes of the political spectrum these anarchist and neo-Nazi/white supremacist channels have tens of thousands of subscribers.

TELEGRAM does not derive any of its operating revenue from advertisements – and that fact alone should raise serious questions who and what is sustaining its platform since it is a free download in these app stores.

TELEGRAM came onto our radar in 2017 when I along with a small group of web terror detectors determined that it had been hijacked by ISIS to organize terrorist plots, disseminate propaganda, and claim responsibility for its global attacks. We uncovered a treasure trove of ISIS accounts which were simultaneously linked to mainstream social media accounts.

Why is TELEGRAM preferred over other encrypted-enabled APPS such as WhatsApp or Signal?

Unlike SIGNAL and WhatsApp, and Wickr (the three other most prominent encrypted-enabled communications channels), TELEGRAM is a veritable terrorist's supermarket of services. TELEGRAM enables extremists to jump between accounts to publish traks and propaganda, solicit donations, issue real-time encrypted instructions, and engage in secure one-on-one and group chats. Most importantly for extremists, TELEGRAM's encryption service is harder for authorities to hack than the encryption technologies found in SIGNAL and WhatsApp

While we were reviewing these intercepts, we also began uncovering Eastern European-based white extremists groups darting in and out of encrypted communications which migrated back and forth onto Facebook Groups, Instagram, and Twitter accounts,

Our research mirrored the excellent research conducted by HATEWATCH – a division of the Southern Poverty Law Center and other concerned organizations.

Alarm bells sounded as other watchdog groups similarly uncovered how prevalent TELEGRAM communications are enabling incitement and violence.

On June 3, 2020 CSW issued a press release proposing a new public safety campaign to hold TELEGRAM's management accountable for enabling anti-Semitic and anti-Black violence in the wake of the murder of George Floyd. Our release cited specific examples of the malicious TELEGRAM-hosted activity.

Then on June 18, 2020, CSW issued another report disclosing that Eastern European and Russian-based white nationalist groups – some linked to the Russian Government's Internet Research Agency – continue to incite racial violence during BLM protests via TELEGRAM.

Our investigation also revealed that Russian-supported white nationalist groups based in St. Petersburg are being directly supported by the Kremlin or are receiving support to operate from St. Petersburg, including the next generation of members of "The Base." These Russian-originating trolls are dispatching racist and anti-Semitic content via so-called feeder TELEGRAM accounts based in Hungary, Belarus, Ukraine, and Estonia.

Finally, on July 22, 2020, CSW a third report revealing that it had uncovered dozens of TELEGRAM messages from both right-wing groups and ANTIFA ideologues recruiting individuals in Portland, OR to engage in violent protests against federal authorities and local police. Many of these intercepts hijacked the "BlackLivesMatter" hashtag and its variations, such as "Strike Force #BLM.

These three reports which provide representative links confirming our collective findings.

Like the SPLC, CSW notified tech companies and the UAE that TELEGRAM was promoting violence and racial incitement:

- **On June 19, 2020, CSW sent a letter to UAE Ambassador to the U.S. H.E. Yousef Al Otaiba to convey our concern about the UAE hosting TELEGRAM's owner and management since it is facilitating terrorist incitement in the U.S. and in Europe with impunity. We have not received any response from the UAE Embassy despite several follow-up requests to his staff. Attached is a copy of CSW's letter.**

- **On July 24, CSW wrote to Apple CEO Tim Cook requesting that he honor his pledge to the Anti-Defamation League by temporarily de-platforming the TLEGRAM App until its owner and management verifiably restrict the use of TELEGRAM as an extremist web weapon.**

  We reminded Mr. Cook when he accepted the Anti-Defamation League's "Courage Against Hate" award in 2018, he stated:

  > **"We only have one message for those who see to push hate, division, and violence. You have no place on our platforms."**

- **On July 30, CSW dispatched a comparable letter to Google's CEO Sundar Pichai.**

So far, CSW has not had the benefit of a reply from either Apple or Google.

What can Congress do about TELEGRAM and its owner/management based in Dubai?

First, I urge the Subcommittee to communicate directly with the government of the UAE to advise it of its deep concern regarding the pernicious role a company based in Dubai has in dispersing anti-Semitic and racial bigotry in the name of terrorist incitement and interfering increasingly in U.S. domestic politics. TELEGRAM was previously booted out of Ireland and was compelled to reduce its presence in the UK for enabling known terrorists to utilize it. Surely, pressure on the UAE to compel TELEGRAM to act against white supremacists and anarchists or risk losing its Dubai haven would get the attention of its owner and management.

Second, I urge the Subcommittee to urge Apple and Google to de-platform TELEGRAM from their app stores until it verifiably shuts down these extremist accounts is the type of corporate boycott which is reasonable and in the interest of public security.

THE ROLE OF QANON IN RADICALIZING AMERICANS

President Trump recently praised the sprawling, bizarre, and baseless QAnon conspiracy which the FBI labeled a domestic terrorist threat last year. According to a BuzzFeed report dated August 19, 2020, Mr. Trump retweeted content from at least 200 QAnon-affiliated accounts.

The President's embrace of the pro-Trump QAnon conspiracists could be brushed aside as just another example of Mr. Trump's penchant to embrace anyone who embraces him – no matter how radical their belief. But his dalliance with QAnon represents the tip of the iceberg. In a sordid tale of dangerous extremist incitement instigated by QAnon followers they "crowd source" their various social media accounts with a treasure trove of crackpot radical beliefs all fed by a torrent of disinformation and misinformation contagion from Kremlin trolls and trans-national white supremacist groups – based in Germany and Russia.

Make no mistake about it, QAnon is inherently anti-Semitic. There are 200,000 QAnon social media accounts tied to German neo-Nazi groups. References to the "Elders of Zion" blood libel and to a "Zionist Occupied Government" are common on QAnon forums according to CSW VP Feinberg in a Jewish Telegraphic Agency interview on September 18, 2020.

According to a West Point Combatting Terrorism Center Report dated July, 2020, QAnon can be thus described:

What is the QAnon Conspiracy?

The QAnon conspiracy[5] emerged on Saturday, October 28, 2017, on 4chan's[a] /pol/ (politically incorrect page) in a thread called "Calm Before the Storm," when an anonymous user signing off as 'Q' stated that "Hillary Clinton will be arrested between 7:45 AM – 8:30 AM EST on Monday the morning on Oct 30, 2017."[6] Q's nom de plume is in reference to "Q" clearance, a clearance level in the United States Department of Energy.

However, QAnon finds its origins a year prior in the Pizzagate conspiracy theory,[7] which alleges coded words and satanic symbolism purportedly apparent in John Podesta's emails, hacked during his tenure as chair of Hillary Clinton's 2016 U.S. presidential campaign, point to a secret child sex trafficking ring at a pizza restaurant in Washington, D.C., called Comet Ping Pong. P Pizzagate came to a head in December 2016 when Edgar M. Welch (whose case is discussed in detail below) traveled from North Carolina "to the popular DC pizzeria Comet Ping Pong with a handgun and an assault rifle to 'self-investigate' the validity of the 4chan conspiracy."[8] QAnon, beginning in 2017, thus originated out of the Pizzagate conspiracy theory, retaining the central belief that a cabal of powerful elites control the world, using their power to covertly abuse children.

Q's claim on 4chan to have special government access and that he/she is part of a wider "anon genre" of government officials with top secret information is not entirely novel. Before Q, several 4chan posters asserted they had special government access, including FBIAnon[9] and HLIAnon[10] in 2016, and CIAAnon[11] and WHInsiderAnon[12] in 2017. QAnon devotees, many of whom may be familiar with this "anon genre," thus are familiar with Q's apparent need for anonymity and presumably take it as a sign of credibility."

The danger posed by this development is well documented.

The FBI named QAnon specifically in a May 2019 intelligence bulletin produced for distribution among intelligence and law enforcement agencies that described "conspiracy theory-driven domestic extremists" as a growing threat in the United States.

Aside from the notorious Pizzagate attack on the DC Comet Pizza restaurant by Edgar Welch in 2016, the FBI has documented arrests which should highlight how QAnon motivates individuals to plot acts of domestic terrorism – in one instance a plot to assassinate Democratic Presidential nominee Joe Biden.

On April 29, 2020, the FBI arrested Jessica Prim for plotting to assassinate VP Biden. Prim – a former stripper from Illinois, who had driven to New York City with a car full of knives. Prim livestreamed her two-day trip during which she threatened to kill VP Biden. Prim first became acquainted with QAnon from Facebook posts in early April. Accordingly, it took just 20 days from her first QAnon introduction to her arrest.

Although QAnon conspiracists latch on to a basic tenet that Donald Trump is fighting a "deep state" conspiracy to prevent him from exposing a cabal of Democratic and Hollywood A-lister pedophiles, what emerges is a strong undercurrent of anti-Semitic bigotry and incitement.

Consequently, social media companies pledged to de-platform most QAnon accounts.

Facebook announced on August 19 it was banning groups and accounts associated with QAnon as well as a variety of U.S.-based militia and anarchist groups that support violence. With one absurd caveat: it would continue to allow people to post material that supports these groups, so long as they do not violate policies against hate speech, abuse, and other provocations.

CSW decided to investigate how well Facebook was adhering to his new anti-QAnon policy.

On September 1, 2020, CSW issued a report stating that despite claims by Facebook and other social media websites they are carefully culling their platforms from extremist QAnon accounts which allegedly violate new policy guardrails, QAnon accounts inciting anti-Semitic and racial bigotry are evading web scrubs by creating new websites, new "#" hashtags, and cross-linking QAnon accounts to white extremist websites, including the websites of many Republican Congressional candidates.

The loophole Facebook created has enabled QAnon adherents to create innocuous sounding accounts focused on a montage of "save the children" hashtags. Why? Facebook's own algorithm amplification (known as "Related Pages") continues to push QAnon supporter accounts to land on new QAnon pages.

Remember, the more the algorithm amplification the more ad revenue.

Moreover, American, and European neo-Nazi white nationalist extremist groups have come upon a recruiting bonanza with the emergence of QAnon. CSW uncovered dozens of previously de-platformed QAnon Facebook accounts with flagrantly anti-Semitic neo-Nazi content correlated across the internet spectrum bouncing around like digital ping-pong balls from Facebook, Twitter, Instagram, GAB, TELEGRAM, and 8kun.

<u>QAnon Accounts Benefit from Extremist White Nationalist Webmasters</u>

CSW uncovered the role played by a MJC (name withheld) from Kentucky who is registering new QAnon websites, including "Birthofanation" located on a new Facebook page: "WWWG1WWG Birthofanation.us" MJC has prior ties to the John Birch Society and the Klu Klux Klan.

As I will discuss in my oral testimony, Congress should commence an investigation into the role played by back-of-the-house web, financial tech, and domain hosting services enabling extremist platforms to operate – many piggybacking onto a misbegotten legal theory that they, too, are immune from any content liability under Section 230 of the CDA.

In a few days, CSW will jointly issue a new report detailing how neo-Nazi groups based in Germany and Eastern Europe are using PayPal and credit and debit card services from Mastercard and Visa to sell their wares.

IS CONGRESS CAUGHT BETWEEN A ROCK & A HARD PLACE? THE CASE FOR A NEW SOCIAL MEDIA STANDARDS BOARD

As this Subcommittee well knows the fate of Section 230 of the CDA is the proverbial elephant in the room, hovering over a potential prescriptive roadmap to end the stalemate between the moral and legal obligation of social media companies to clean up their platforms.

CSW is on record urging Congress for the sake of our democracy and the safety of the American people, to end the immunity from content liability accorded social media companies, which has, by judicial extension, enabled fringe web supported radical and extremist websites to also claim the same immunity from content liability.

But we are realists and we simply do not envision in the foreseeable future a bi-partisan agreement to achieve this objective – even splitting off from content immunity the extremist incitement rags which pass as websites, including GAB, 4chan, 8kun, and the other scum of social media catering to terrorists and funneling Russian disinformation and misinformation into our political discourse.

That is why CSW developed a public/private sector solution to tackle this dilemma – a new Social Media Standards Board (SMSB).

The SMSB would serve as a:

- **Transparent content moderation auditing organization to monitor compliance by social media companies of a new industry "code of conduct" developed with the participation of concerned citizens groups, social media companies, and the advertising industry – which is, after all, the industry with the most leverage over social media and which created a new Global Alliance for Responsible Media (GARM) to accomplish this goal.**

- **Forum to incubate and promote new technologies to assist social media companies to fulfill their own customer and vendor obligations to better manage and achieve verifiable commitments to de-platform extremist incitement, dis, and misinformation.**

The SMSB is loosely modeled after the successful 1973 banking industry's Financial Accounting Standards Board (FASB), which was created precisely to harmonize the various standards (think customer terms of service) of banks and develop private sector regulatory mechanisms to hold banks to their industry and regulatory commitments.

The following is extracted from CSW's SMSB proposal dated August 20, 2020 and attached to my testimony, which was also the subject of an article published in The Hill.

It envisions passage by Congress of an amendment to Section 230 delegating to the SMSB the power to suspend Section 230 immunity until a violating social media company restores its compliance with new industry code of conduct. The loss of Section 230 immunity would represent the ultimate penalty imposed on code violators for sustained violations. Lesser sanctions against social media companies imposed by the SMSB code could conceivably include: 1) de-certification from code compliance; 2) forfeiture of digital ad revenue; and 3) a referral by the SMSB for administrative action to the Federal Trade Commission.

Should the Subcommittee consider a SMSB worthy of further consideration I hope it will invite to testify representatives of GARM to discuss how the digital advertising industry intends to use its undeniable financial leverage it has to compel social media companies to abide by verifiable standards which protect their brand safety both in the United States and abroad.

Thank you and I look forward to responding to your questions and assisting the Subcommittee members and their staff in the weeks and months ahead.

==========