Tech has made a number of ambitious claims about the ability of machine learning and artificial intelligence (AI) to identify terrorist content. Tech also frequently refers to its industry 'hashing database' which purports to contain a set of hashes of terrorist material that is shared across the industry. In 2017, your companies led the creation of the Global Internet Forum to Counter Terrorism (GIFCT) to coordinate the industry's response to the misuse of Internet platforms by extremist and terrorist actors. The GIFCT's stated mission was to leverage technology and share information and best practices with all member companies, especially through a shared industry hash database. However, at a January 2018 Senate Commerce Committee hearing, company officials acknowledged the failure to agree on a common standard for prohibited extremist and terrorist content. And this year, this 'hash database' failed to stop millions of copies of the New Zealand attacker's video spreading across yours and other companies' platforms.

- Since last January, has the GIFCT adopted a standard for prohibited content that is hashed and stored on the shared database?
- Since last January, has the GIFCT adopted a standard for prohibited content that is hashed and stored on the shared database?
- Will the GIFCT commit to prohibiting content produced by or on behalf of U.S., E.U. and/or U.N.-designated individuals and organizations as well as individuals and specific pieces of content with demonstrable links to violence?
- How exactly and how quickly does the GIFCT add new content to the shared hashing database once a member company identifies and removes it? How exactly and how quickly – if at all – do individual companies hash GIFCT-hashed content across their own sites and platforms? How much content removed by each GIFCT member company was identified solely via the shared database
- Will your companies and the GIFCT make their hashing database widely available for review by the government and experts in counter-terrorism, counter-extremism and related fields? The GIFCT's transparency will allow lawmakers and the general public to confirm GIFCT's claims about the comprehensiveness, scope and accuracy of the database.

—

The tech industry has been lobbying EU lawmakers to water down proposed regulations that would require tech firms to remove flagged content within one hour. Specifically, tech lobbyists claim one hour is too burdensome and will hurt small and medium sized enterprises (SMEs). However, a stated objective of the GIFCT is to leverage technology as well as share information and best practices with members. Why aren't the larger tech firms assisting smaller companies (i.e. providing them with resources, technology, etc.) to help offset costs of compliance? Isn't this one of the principal promises of the GIFCT?

—

The majority of the technology industry's public-facing representatives are lawyers and public relations professionals – or so-called "policy professionals." However, the systems in question and the methods meant to control and police them are developed by engineers, computer scientists and digital forensics experts. Isn't it time we hear directly from the subject-matter experts designing and implementing your efforts to take down extremist content from your platforms? Will you commit today to making your technological experts available to testify and address our questions and concerns?

—

Facebook CEO Mark Zuckerberg recently wrote a widely-publicized op-ed and appeared on Good Morning America calling for government regulation of online platforms and content. However, he did not offer a single specific policy proposal. The Communications Decency Act continues to shield tech companies from liability for content posted to their platforms by third parties, including content from white nationalists and other extremists that displays, glorifies or incites violence. But the Internet has grown and changed dramatically since the law was passed 21 years ago. Tech companies now create and manipulate their own television shows and movies, produce and disseminate news programming, recommend and/or promote certain content over others, consult political campaigns and of course aggregate the information shared on their platforms for the purpose of monetization via advertising.

- Given this 'activist' role in the production, promotion and manipulation of media content, will your company support lawmakers in removing social media companies' blanket CDA Section 230 protections from liability for harmful content?
- If not, how can you still claim to be a neutral third-party content host?

—

It is clear that tech giants cannot be trusted to share information or enforce their own policies. Will Facebook and Google support amending Securities Laws governing the Securities and Exchange Commission (SEC) to require that publicly traded Internet companies file SEC reports on how much extremist content exists on these platforms as well as the efficacy of their removal efforts? Releasing the information is a responsibility companies have not only to the general public, but also to their shareholders.

—

Earlier this year, YouTube was found allowing the upload of an audiobook of a neo-Nazi manifesto, Siege, and enabling it to accumulate thousands of views. The book calls for followers to commit violence against the U.S. government, incite race wars and kill Jews and people of mixed race. When asked to take down said content, a YouTube spokesperson stated that a simple warning that played before the video was proof of Google and YouTube's "tougher stance on videos that are borderline against our policies on hate speech and violent extremism." The spokesman further said allowing the video with a warning struck "a good balance between allowing free expression and limiting affected videos' ability to be widely promoted on YouTube."

- Will YouTube revisit its policy on content posted by white nationalists or supremacists that shows, glorifies or incites violence?
- How did YouTube determine that a violent manifesto like Siege could be permitted on its platform, but not different versions and variations of the New Zealand terrorist's video and 74-page manifesto?
- How many such white supremacist, nationalist and neo-Nazi videos does YouTube currently host on its platform in keeping with its commitment to 'free expression'?
- Will YouTube continue allowing said content on its platform now that it has led to yet another violent attack in the real world?

—

Last year, Facebook CEO Mark Zuckerberg testified before the U.S. Senate Judiciary Committee and claimed the company's algorithms and AI were able to remove 99 percent of all ISIS and al-Qaeda content. This year, Facebook CTO Mike Schroepfer said AI technology has an approximate accuracy rate of 90 percent. Then, in a series of paid articles in The Telegraph touting Facebook's "mix of solutions" targeting extremist content, members of your Counter-Terrorism and Dangerous Organizations Team said 83 percent of terrorist content is removed within the hour if it is previously identified and flagged. Now, you claim to have difficulty differentiating between terrorist content and "visually similar" content after the New Zealand terrorist attack.

- Have Mr. Zuckerberg and Mr. Schroepfer been misrepresenting your company's ability to monitor and remove extremist content?
- What percent of the New Zealand terrorist's videos have you removed using AI compared to human flaggers?
- How many times have similar white nationalist, separatist, and supremacist videos evaded your algorithms and artificial intelligence systems in the past, and for how long?

—

In 2017, after years of CEP advocacy, the New York Times reported that in a "watershed moment," YouTube made the company-wide decision to categorize Anwar al-Awlaki, a radical Islamist and al-Qaeda operative, the same way it categorized terrorist organizations and enacted a "near-total ban" on videos of him. According to company officials, YouTube's technology and human reviewers would work together to automatically flag Awlaki's videos and block them before users could see them. The technology would then create a digital fingerprint of the blocked video to automatically prevent any future uploads of copies.

- Why has YouTube failed to enact similar bans on other notorious extremists or organizations – especially those on U.S., E.U. and U.N. sanctions lists – in the two years since?
- For example, CEP has flagged numerous examples of online content from Yusuf al-Qaradawi, Abdullah al-Faisal and Ahmad Musa Jibril, as well as content with demonstrable links to violence such as Siege and the Turner Diaries. Is YouTube unable, unwilling or both?

—

Pro Publica reported in 2017 that Facebook acknowledged that out of a selection of 49 posts that included hate speech, your content reviewers had wrongly left almost half of them online. You left up a page entitled “Jewish Ritual Murder” even after the Anti-Defamation League flagged it. Given the Christchurch attack, it’s chilling that you left up an image that said, “the only good Muslim is a f***ing dead one.” You always apologize for your shortcomings, promise to do better, and make vague statements of support for some kind of regulation, but you end up opposing concrete regulatory proposals like a pending one in the European Parliament, and these attacks happen again and again. When will you drop your opposition to and relentless lobbying against reasonable regulations, and adopt hashing software that would keep prohibited content from being re-uploaded time and time again?

—

In 2018, the New York Times reported that Facebook was leaving up posts that showed, glorified or incited violence against the Muslim minority population in Sri Lanka. Quote: “A reconstruction of Sri Lanka’s descent into violence, based on interviews with officials, victims and ordinary users caught up in online anger, found that Facebook’s newsfeed played a central role in nearly every step from rumor to killing. Facebook officials, they say, ignored repeated warnings of the potential for violence, resisting pressure to hire moderators or establish emergency points of contact.” Instead of just apologizing for your failure to prevent killing of Muslims in Sri Lanka facilitated by your platform, will you finally support specific U.S. and foreign regulations that will remove your immunity from liability for such content, require you to take it down once governments tell you about it and use technology that prevents such violent content from being re-uploaded over and over again?