28 July 2020

Dear Mr. Rasmussen,

We, the undersigned organizations, are writing to apprise you of shared civil society concerns and perspectives on the reorganization of the Global Internet Forum to Counter Terrorism ('GIFCT') and its work moving forward. Over the past few years, many of us have discussed our concerns with the GIFCT's founding companies about the growing role of the GIFCT in regulating content online. We have enclosed a letter that a number of civil society organisations sent to those companies in February outlining these concerns, including risks of extra-legal censorship from government participation in the Independent Advisory Committee ('IAC'), increasing use and scope of the hash database and persistent lack of transparency around GIFCT activity. We also highlighted a number of issues with the mandate and structure of the IAC itself, including its lack of focus on the protection of human rights—a key component in countering terrorism—as well as an uneven playing field that disadvantages civil society, and lack of structural independence for NGOs.

In our February 25 letter, we made a number of detailed recommendations on how to address these concerns. We chose not to apply to participate in the IAC because these concerns have not yet been addressed, including in the April 3 private communication from the Interim Executive Director of GIFCT. This suggested to us that GIFCT may not be responsive to our concerns and that civil society participation would create the perception of input without actually addressing our substantive issues or suggestions. Genuine multi-stakeholder engagement requires sustained, honest, responsive engagement with the concerns raised by civil society.

As noted in your own terms of reference, the recently announced IAC is meant to, amongst other things, "[e]nsure that GIFCT's work is aligned with international human rights laws," and to promote transparency and accountability. This won't be possible without being open and responsive to critique from human rights experts. However, GIFCT's prior lack of responsiveness to our critiques informed our decision to not apply to join the IAC, thus leaving the IAC composed almost entirely of government officials and academics.

Despite our choice to not join the IAC, we remain committed to addressing the issues we have raised. Some of our organizations will be participating in Working Groups because it is clear to us that GIFCT is taking an increasingly large role globally that could threaten

human rights and we have valuable expertise we can contribute to the focus areas of the Working Groups despite our concerns outlined above.

We write to alert you to these issues and to ask that you meet with us to discuss your plans moving forward.

We would also like to discuss your vision for GIFCT and where you see it fitting into existing content moderation and counter-terrorism work. In a troubling trend, policy makers in government and at technology companies are increasingly treating content moderation as the tool of choice for counter-terrorism work without any assessment of its impact on human rights, much less adequate safeguards for protection of those rights. Content moderation also appears to be deployed at the expense of other programmes that could address the root causes of "violent extremism" and radicalisation more effectively in the long term. GIFCT is also engaging with law enforcement and experts in challenging violent extremism and counter-terrorism without transparency or any real assessment of the potential human rights harms this could cause. Counter-terrorism programs and surveillance have violated the rights of Muslims, Arabs, and other groups around the world, and have been used by governments to silence civil society.[1] We want to ensure that the boundaries between content moderation and counter terrorism are clear.

Now, as GIFCT member companies increasingly use machine learning algorithms to detect and remove content, mistakes are being made. There is evidence that processes intended to remove terrorist content have the counter-productive effect of removing anti-terrorism counterspeech, satire, journalistic material, and other content that would, under most democratic legal frameworks, be considered legitimate speech. In particular, documentation of human rights abuses is disappearing at an astonishing rate.[2] This hampers journalism and humanitarian work, and jeopardizes the future ability of judicial mechanisms to provide remedy for victims and accountability for perpetrators of serious

---

[1] *See, e.g.,* United Nations Human Rights Council, *Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders - Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* A/HRC/40/52, 1 Mar 2019, *available at* https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/40/52; Center for Consitutiuonal Rights, *Muslim Profiling,* https://ccrjustice.org/home/what-we-do/issues/muslim-profiling (last visited 21 Jul. 2020)
[2] *See, e.g.,* Abdul Rahman Al Jaloud et al, *Caught in the Net: The Impact of "Extremist" Speech Regulations on Human Rights Content*, Electronic Frontier Foundation, Syrian Archive, and WITNESS, 30 May 2019, *available at* https://www.eff.org/wp/caught-net-impact-extremist-speech-regulations-human-rights-content; Syrian Archive, *Lost and Found: Syrian Archive's work on content taken down from social media platforms,* https://syrianarchive.org/en/lost-found (last updated 11 Jun. 2020)

crimes such as genocide.[3] The removal of content that is potentially valuable evidence is particularly prevalent in relation to conflicts in predominantly Muslim and Arabic-speaking countries such as Syria and Yemen—the same communities that have already seen their rights violated in the name of countering terrorism. We would like to hear your views on these issues and on how you intend to preserve valuable evidence in a manner that addresses both privacy rights and the need for accountability.

In your former capacity as a US government official, you've also spoken about the dangers that encryption poses to national security. We would like to hear how you now view encryption, particularly in light of its use by human rights defenders around the world who face risks to life and liberty should their communications fall into the wrong hands.

Finally, in recent years you've made it clear that, at least in the United States, you see right-wing violent extremism as a key threat. Recent work on content moderation, such as the Christchurch Call, has largely been spurred by violent acts committed by individuals espousing this type of ideology. The Christchurch Call was, of course, a response to the Christchurch massacre on March 15, 2019, when a white supremacist gunman murdered 51 Muslims during prayer. Yet GIFCT, which was bolstered institutionally in response to the Christchurch massacre, continues to operate in a complex global environment that lacks internationally agreed upon definitions of terrorism or extremist violence, where such right-wing violent extremism is by and large not legally recognized.

Without a common definition for either "terrorism" or "violent extremism," the formulation and enforcement of rules against such content can only be seen as highly subjective and potentially biased. This is a greater problem than GIFCT alone can address, of course. Nonetheless, we caution against building a content moderation framework on such a foundation. Given your demonstrated understanding of the spectrum of extremist violent threats, we would welcome your thoughts on how GIFCT should approach this dilemma.

Below our signatures is the full text of our February letter. Please note that the lists of signatories for that letter and the present one are not identical, though there is overlap. We look forward to engaging with you on these critically important issues and would

---

[3] *Id.*; Raja Althabani et. al, *Digital Video Evidence, When Collected, Verified, Stored, and Deployed Properly, Presents New Opportunities for Justice,* International Criminal Court Forum, 1 Jun. 2020, https://iccforum.com/cyber-evidence#Kayyali ; Alexa Koenig, *Digital and Open Source Information Can Play a Critical Role in Improving the Overall Efficiency and Efficacy of the International Criminal Court*, International Criminal Court Forum, 1 Jun. 2020, https://iccforum.com/cyber-evidence#Koenig

welcome the opportunity to discuss them in a call or virtual meeting as soon as your schedule permits.

Sincerely yours,

Access Now
ARTICLE 19
Association for Progressive Communications
BlueLink
Center for Democracy & Technology
Committee to Protect Journalists
Dangerous Speech Project
Derechos Digitales
Electronic Frontier Foundation
Human Rights Watch
Privacy International
Ranking Digital Rights
Rights and Security International
SMEX
Syrian Archive
WITNESS

Dear [Representatives from Facebook, Google, Microsoft, and Twitter]

We, the undersigned organizations, are writing in response to the Global Internet Forum to Counter Terrorism ('GIFCT') call for expressions of interest to join its Independent Advisory Committee (IAC). As human rights and civil liberties organizations, many of us have engaged with your companies and through GIFCT convenings over the past few years in the spirit of open and honest exchange, with the goal of promoting fundamental human rights and ensuring accountability for governmental and corporate actors alike.

In that same spirit, we write today to share some of our key concerns about the IAC specifically, and the growing role of GIFCT more broadly in regulating content online. Many of our organizations have discussed concerns with you over the past few years, including our deep skepticism about the creation of a shared hash database and the risks involved in content removal coordination among companies; the lack of clarity over how GIFCT defines or distinguishes "terrorism," "violent extremism," "extremism," and support for or incitement to them; increasing reference by governments to GIFCT as a quasi-official body. Unfortunately, we have yet to see GIFCT genuinely address these issues. In fact, unless GIFCT significantly changes course now to address the concerns we lay out below, we believe participation of civil society on the IAC will be window-dressing for the real threats to human rights posed by GIFCT. For these and other reasons, our organizations will not apply for membership in the IAC at this time.

Extralegal censorship from government involvement in GIFCT
We have always been concerned that GIFCT—even though framed to us as a voluntary, industry-only entity—would ultimately be vested with some kind of governmental authority or otherwise entangled with state actors. This appears to have happened with the formalisation of the IAC and its inclusion of governments as members. Governments will almost certainly use their influence in GIFCT to further leverage member companies' "Community Guidelines" and content moderation policies as a way to secure global removal of speech.

This would not only significantly undermine formal mechanisms to hold governments and companies to account, it will also inevitably lead to greater censorship of protected speech, hinder independent journalism and research, and bury or destroy evidence that could lead to war crimes prosecutions. We know from years of experience and evidence that GIFCT members already remove significant amounts of protected speech under their "Community Guidelines" by using broad definitions of what constitutes, for example, "support for violent extremism," as well as by relying upon lists issued by national

governments to determine affiliation with terrorist organizations.[4] We are deeply concerned that increasing government influence on "Community Guidelines"-based removals will result in further weakening of users' freedom of expression.

Increasing scope and use of shared hash database

Even prior to the launch of GIFCT in 2017, the launch of the shared hash database in December 2016 prompted many of our organizations to raise concerns about the existence of a centralized resource focused on content removal across platforms.[5] Such a centralized repository, based on the contributions of individual companies according to their own idiosyncratic definitions of "terrorist" content, risks creating a lowest-common-denominator definition of "terrorism" and perpetuates the incorrect notion that there exists a global consensus on the meanings of "terrorist" and "violent extremist" content. Moreover, we are concerned that the definitions and taxonomy used to populate the database have been applied in a discriminatory manner. While the GIFCT's profile was raised significantly by the Christchurch Call—itself a reaction to a white supremacist attack on Christchurch's Muslim community—we have not seen any indication that GIFCT's focus goes beyond what it considers to be Islamist-linked violent extremist or terrorist content.

While we understand that each participating company retains the right to make individualized decisions about whether to remove any particular post from its service on the basis of its own definition of these terms, in practice we are concerned that small companies will use the database to automate removal because they do not have the resources to carry out individualized reviews. We also understand that even the largest companies sometimes automate content removal decisions.[6] This has resulted and will continue to result in the destruction of evidence of war crimes and the stifling of critical expression, including speech challenging government policies, corporations, and violent

---

[4] *See, e.g.,* Abdul Rahman Al Jaloud et al, *Caught in the Net: The Impact of "Extremist" Speech Regulations on Human Rights Content*, Electronic Frontier Foundation, Syrian Archive, and WITNESS, 30 May 2019, *available at* https://www.eff.org/wp/caught-net-impact-extremist-speech-regulations-human-rights-content. (Describing removals of documentation of conflicts in Syria, Yemen, and Ukraine, and noting that lists used by companies to determine what content should be removed tend to reflect the political biases of the governments that construct them.)

[5] Emma Llansó, *Takedown Collaboration by Private Companies Creates Troubling Precedent,* Center for Democracy and Technology, 6 Dec 2016, https://cdt.org/insights/takedown-collaboration-by-private-companies-creates-troubling-precedent/

[6] Elizabeth Dwoskin and Craig Timberg, *Inside YouTube's struggles to shut down video of the New Zealand shooting — and the humans who outsmarted its systems,* Washington Post, 18 Mar 2019, https://www.washingtonpost.com/technology/2019/03/18/inside-youtubes-struggles-shut-down-video-new-zealand-shooting-humans-who-outsmarted-its-systems/

extremism.[7] Even when humans are involved in reviewing content, companies' moderation systems have often proven unable to distinguish the nuance between material that constitutes incitement to terrorism and legitimate reporting on human rights abuses.

Persistent lack of transparency around GIFCT activity
Many of our organizations have called on GIFCT and its member companies to increase public transparency about its membership, activities, and relationship with governments.[8] We welcomed the first GIFCT transparency report published last year, but GIFCT must publish more detailed and meaningful information on a regular basis, particularly as it formalizes its relationship with government officials. We emphasize that transparency to the IAC alone is insufficient; decisions made by GIFCT member companies affect individuals and communities around the world.

In addition to our concerns about the very existence of the shared hash database, many of our organizations have repeatedly highlighted shortcomings in transparency around it. There is little visibility to anyone outside of the GIFCT member companies as to what content is represented in the hash database. We understand that the shared hash database is a collection of hashes and not itself a repository of content that could be reviewed. This, however, is not an answer to the underlying concern that GIFCT is maintaining a shared content removal resource that cannot be objectively evaluated to determine whether, for example, protected speech is being censored, or evidence of war crimes or other valuable evidence is being destroyed.

Independence and role of NGOs
We also have several concerns relating to the GIFCT/IAC and our role as NGOs. We deeply value our independence and ability to speak publicly on a host of issues, including human rights, the rule of law, governance, and the impact of technology on society. Sitting with governments on the IAC could compromise our ability to do so, as

---

[7] *See, e.g.*, Al Jaloud et al, supra note 1.

[8] Dia Kayyali, *WITNESS tells world leaders- don't delete opportunities for justice,* WITNESS, 24 Sep 2019, https://blog.witness.org/2019/09/witness-tells-world-leaders-dont-delete-opportunities-justice/; Jillian York, *The Christchurch Call Comes to the UN,* EFF, 26 Sep 2019, https://www.eff.org/deeplinks/2019/09/christchurch-call; Dia Kayyali, *Human rights defenders are not terrorists, and their content is not propaganda*, WITNESS, 21 Jan 2020, https://blog.witness.org/2020/01/human-rights-defenders-not-terrorists-content-not-propaganda/; *Civil Society Letter to Members of the European Parliament on Concerns with Terrorism Hash Database* 4 Feb 2019, *available at* https://cdt.org/insights/letter-to-members-of-the-european-parliament-on-concerns-with-terrorism-hash-database/.

some NGOs may receive funding from governments on the IAC or face surveillance or threats of reprisals from them.

Another concern is that the power dynamics between government officials, including law enforcement, and individuals representing civil society organizations will place our interactions on inherently unequal footing. Our experience with multi-stakeholder initiatives that involve the private sector, civil society, and governments is varied, but when companies act in an opaque and deferential manner towards government officials in these contexts, governments can wield extraordinary influence on the outcomes of these initiatives. Indeed, this has been our experience with GIFCT thus far: governments have been directly involved in the negotiations about the future of the GIFCT, while civil society has been relegated to a barely consulted afterthought. This dynamic can make it very difficult to prevent, modify, or reverse decisions that harm human rights or to hold governments accountable for the policies or actions they promote. We are concerned that the IAC structure will only increase governments' influence over GIFCT.

In our view, for GIFCT to be regarded as a credible entity that seeks to protect human rights, its members should at the very least:

- *Conduct and share publicly an independent assessment of the risks to freedom of expression and other human rights that stem from GIFCT, including those related to its not-for-profit status. This assessment should include:*
  - *A thorough analysis of the legal landscape(s) in which GIFCT will operate, including laws that may compel GIFCT to disclose user data;*
  - *An analysis of the human rights risks of:*
    - *Government pressure and influence on participating companies to remove lawful content under their content moderation policies;*
    - *Use of overly broad and discriminatory criteria for removing "terrorist" or "extremist" content;*
    - *Use of hash-matching as a means for identifying content for automated removal or human review;*
    - *The lack of transparency about the contents and operation of the hash database;*
    - *GIFCT's potential relationships with governments and other entities; and*
  - *A plan setting out how GIFCT will mitigate any identified risks, including through a credible and effective process to ensure that actions can be remedied if they harm rights.*

- *Commit to accepting an independent, external audit or review of the content represented in the hash database, and take whatever steps are necessary to do so, including creating a continually updated repository, or asking member companies to do so individually, of the material the hash database reflects.*

- *Prioritize making information publicly available about GIFCT's practices, including the operation of and content reflected in the hash database.[9]*

We share these concerns and recommendations with you in a spirit of candor and with the goal of continued dialogue. We know these are complex challenges and that the global environment for freedom of expression and preserving an open Internet is more fraught than ever.

Sincerely,
Access Now
Amnesty International
ARTICLE 19
Association for Progressive Communications (APC)
BlueLink Foundation
Center for Democracy & Technology
Committee to Protect Journalists
Dangerous Speech Project
Derechos Digitales
Electronic Frontier Foundation
Human Rights Watch
International Commission of Jurists
Privacy International
Ranking Digital Rights
Rights Watch (UK)
SMEX
Syrian Archive
WITNESS

---

[9] *See, e.g.*, Llansó *supra* note 2 (for a list of specific transparency recommendations)