



GIFCT

Global Internet Forum
to Counter Terrorism

Transparency Recommendations for GIFCT

Prepared by the GIFCT
Transparency Working Group

June 2021



GIFCT
Global Internet Forum
to Counter Terrorism



Introduction

The Global Internet Forum to Counter Terrorism (GIFCT) Transparency Working Group (WG) was established in April 2020 as part of the GIFCT substantive Working Group structure. The Transparency WG's objective is to develop best practices and easy access to resources that facilitate greater transparency from all relevant stakeholders while respecting privacy and human rights. Microsoft and Organization for Economic Co-operation and Development (OECD) representatives serve as co-leads for the WG.

In support of its objective, a priority output for the WG is to provide recommendations to the GIFCT intended to help enhance the transparency of the organization and its activities. This report sets out those recommendations as of June 2021.

Debates such as these will likely grow more pronounced in the future as terrorists and violent extremists from across the ideological spectrum further capitalize on new technologies ranging from cryptocurrency to 3D printing. Counterterrorism efforts, meanwhile, will likely come to rely more heavily on big data and artificial intelligence (AI)-driven technologies, raising various ethical challenges. To prepare for the future of terrorism, one need only to look to the past and see that technological innovations have always been instrumental to acts of terror—and efforts to prevent them.

This white paper maps these continually shifting dynamics, drawing on proceedings from meetings of the GIFCT Academic and Practical Research Working Group, the work of the Global Network on Extremism and Technology (GNET), and original desk research. In doing so, it identifies key emerging trends and research priorities related to violent extremism, counterterrorism, and the role of the internet in these spaces. The paper is divided into three sections that respectively examine innovations in violent extremism, new developments in extremist outreach and messaging, and new research and priorities as they relate to preventing terrorist use of the internet (PTUI).

The GIFCT's approach to transparency

The WG notes that GIFCT has dual functions in facilitating transparency:

- a) By requiring tech companies to develop their own transparency reports as a condition of GIFCT membership and facilitating this through the membership process (whereby companies are supported through Tech Against Terrorism's Mentorship Program); and
- b) To lead by example in establishing best practices for internal transparency, including the provision of information on its website and the production of an annual transparency report. In producing GIFCT's own transparency report, GIFCT should be transparent about its own efforts, both in terms of programs and technical tooling used by members.

In this context, the WG recommends to GIFCT that:

1. GIFCT compile and make more accessible on its website links to its member companies' transparency reporting, terms of service, and other relevant policies and safety information;
2. GIFCT offer greater clarity on the taxonomy used to define terrorist and violent extremist content with reference to the hash-sharing database (discussed further below);
3. GIFCT provide more public information on GIFCT membership and the Tech Against Terrorism mentorship program in order to help potential members understand the process and decision-points. This could include more details on:
 - the membership process and requirements;
 - the number of companies currently in the mentorship program;
 - the timeframes and selection criteria for mentorship and entering the membership process; and
 - how many (if any) companies have been declined GIFCT membership, including the rationale.

It may also be helpful to outline the costs and benefits of GIFCT membership.

Recommendations related to the hash-sharing database

The WG has also discussed the GIFCT hash-sharing database and recommends that:

1. GIFCT provide a clearer narrative and/or more detailed explanation about how hashed content and URLs end up in the databases. This may include the criteria and decision-making processes for determining whether content should be added (including the actors involved, as well as any review and quality control processes), any human rights analysis undertaken, and whether the process is manual or automated. Visualizations could be helpful to explain this to non-tech audiences;
2. GIFCT clarify the purposes for which accredited third parties (such as academics) could be granted access to the database and the process and conditions for granting such access. If these are yet to be determined, the WG recommends GIFCT consult on any such process and conditions, including on the human rights implications and alignment with GIFCT's values;
3. GIFCT recommend that relevant Working Groups consider issues related to human rights and due process in relation to the use of the database;
4. GIFCT facilitate better understanding of how each member company uses the hash-sharing and URL database. Options to implement this could, for instance, include encouraging the inclusion of related text in member transparency reports, or GIFCT collating information on member practices; and
5. GIFCT consider requiring, as a condition of membership, that member companies notify users when their content has been added to the GIFCT hash-database, provide a process for users to appeal such a decision, and offer a remedy in the event of a successful appeal (noting that this may be subject to legal, privacy, or other restrictions). The WG recognizes that this may be a long-term item of work.

Specific recommendations for the GIFCT's Transparency Report

To add clarity to the GIFCT Transparency Report, the WG recommends that:

1. GIFCT use specific language to detail which companies are members, as well as when members joined (this arises from an ambiguity in the 2020 report which says “members include,” suggesting that the list is incomplete);
2. GIFCT provide greater transparency on the criteria for activating the Content Incident Protocol;
3. GIFCT provide (to the extent possible) greater transparency on the contents of the hash-sharing database;
4. GIFCT offer (to the extent possible) detail on any requests to GIFCT for content, data, or other information from governments or law enforcement agencies, including the source of the request, the content, data, or other information sought, and the legal basis (if any) provided to justify the request.

Conclusion

The WG welcomes any feedback from GIFCT on the recommendations in this report, including regarding where it has adopted the recommendations or where these may pose challenges. The WG may provide further recommendations following the release of the next GIFCT Transparency Report (expected in July 2021).

To learn more about the Global Internet
Forum to Counter Terrorism (GIFCT), please
visit our website or email outreach@gifct.org.

