

15 May 2019 - Charte

### The Christchurch Call to Action To Eliminate Terrorist and Violent Extremist Content Online

#### Télécharger le .pdf

A free, open and secure internet is a powerful tool to promote connectivity, enhance social inclusiveness and foster economic growth.

The internet is, however, not immune from abuse by terrorist and violent extremist actors. This was tragically highlighted by the terrorist attacks of 15 March 2019 on the Muslim community of Christchurch – terrorist attacks that were designed to go viral.

The dissemination of such content online has adverse impacts on the human rights of the victims, on our collective security and on people all over the world.

Significant steps have already been taken to address this issue by, among others: the European Commission with initiatives such as the EU Internet Forum; the G20, and the G7, including work underway during France's G7 Presidency on combating the use of the internet for terrorist and violent extremist purposes; along with the Global Internet Forum to Counter Terrorism (GIFCT); the Global Counterterrorism Forum; Tech Against Terrorism; and the Aqaba Process established by the Hashemite Kingdom of Jordan.

The events of Christchurch highlighted once again the urgent need for action and enhanced cooperation among the wide range of actors with influence over this issue, including governments, civil society, and online service providers, such as social media companies, to eliminate terrorist and violent extremist content online.

The Call outlines collective, voluntary commitments from Governments and online service providers intended to address the issue of terrorist and violent extremist content online and to prevent the abuse of the internet as occurred in and after the Christchurch attacks.

All action on this issue must be consistent with principles of a free, open and secure internet, without compromising human rights and fundamental freedoms, including freedom of expression. It must also recognise the internet's ability to act as a force for good, including by promoting innovation and economic development and fostering inclusive societies.

### To that end, we, the Governments, commit to:

Counter the drivers of terrorism and violent extremismby strengthening the resilience and inclusiveness of our societies to enable them to resist terrorist and violent extremist ideologies, including through education, building media literacy to help counter distorted terrorist and violent extremist narratives, and the fight against inequality.

Ensure effective enforcement of applicable laws that prohibit the production or dissemination of terrorist and violent extremist content, in a manner consistent with the rule of law and international human rights law, including freedom of expression.

Encourage media outlets to apply ethical standards when depicting terrorist events online, to avoid amplifying terrorist and violent extremist content.

Support frameworks, such as industry standards, to ensure that reporting on terrorist attacks does not amplify terrorist and violent extremist content, without prejudice to responsible coverage of terrorism and violent

Consider appropriate action to prevent the use of online services to disseminate terrorist and violent extremist content, including through collaborative actions, such as:

- → Awareness-raising and capacity-building activities aimed at smaller online service providers;
- → Development of industry standards or voluntary frameworks;
- → Regulatory or policy measures consistent with a free, open and secure internet and international human rights law.

# To that end, we, the online service providers, commit to:

Take transparent, specific measures seeking to prevent the upload of terrorist and violent extremist content and to prevent its dissemination on social media and similar content-sharing services, including its immediate and permanent removal, without prejudice to law enforcement and user appeals requirements, in a manner consistent with human rights and fundamental freedoms. Cooperative measures to achieve these outcomes may include technology development, the expansion and use of shared databases of hashes and URLs, and effective notice and takedown procedures.

Provide greater transparency in the setting of community standards or terms of service, including by:

- → Outlining and publishing the consequences of sharing terrorist and violent extremist content;
- → Describing policies and putting in place procedures for detecting and removing terrorist and violent extremist content.

Enforce those community standards or terms of service in a manner consistent with human rights and fundamental freedoms, including by:

- → Prioritising moderation of terrorist and violent extremist content, however identified;
- → Closing accounts where appropriate;
- → Providing an efficient complaints and appeals process for those wishing to contest the removal of their content or a decision to decline the upload of their content.

Implement immediate, effective measures to mitigate the specific risk that terrorist and violent extremist content is disseminated through livestreaming, including identification of content for real-time review.

Implement regular and transparent public reporting, in a way that is measurable and supported by clear methodology, on the quantity and nature of terrorist and violent extremist content being detected and removed.

Review the operation of algorithms and other processes that may drive users towards and/or amplify terrorist and violent extremist content to better understand possible intervention points and to implement changes where this occurs. This may include using algorithms and other processes to redirect users from such content or the promotion of credible, positive alternatives or counter-narratives. This may include building appropriate mechanisms for reporting, designed in a multi-stakeholder process and without compromising trade secrets or the effectiveness of service providers' practices through unnecessary disclosure.

Work together to ensure cross-industry efforts are coordinated and robust, for instance by investing in and expanding the GIFCT, and by sharing knowledge and expertise.

## service providers, commit to work collectively to:

Work with civil society to promote community-led efforts to counter violent extremism in all its forms, including through the development and promotion of positive alternatives and counter-messaging.

Develop effective interventions, based on trusted information sharing about the effects of algorithmic and other processes, to redirect users from terrorist and violent extremist content.

Accelerate research into and development of technical solutions to prevent the upload of and to detect and immediately remove terrorist and violent extremist content online, and share these solutions through open channels, drawing on expertise from academia, researchers, and civil society.

Support research and academic efforts to better understand, prevent and counter terrorist and violent extremist content online, including both the offline and online impacts of this activity.

Ensure appropriate cooperation with and among law enforcementagencies for the purposes of investigating and prosecuting illegal online activity in regard to detected and/or removed terrorist and violent extremist content, in a manner consistent with rule of law and human rights protections.

Support smaller platforms as they build capacity to remove terrorist and violent extremist content including through sharing technical solutions and relevant databases of hashes or other relevant material, such as the GIFCT shared database.

Collaborate, and support partner countries, in the development and implementation of best practicein preventing the dissemination of terrorist and violent extremist content online, including through operational coordination and trusted information exchanges in accordance with relevant data protection and privacy rules.

Develop processes allowing governments and online service providers to respond rapidly, effectively and in a coordinated manner to the dissemination of terrorist or violent extremist content following a terrorist event. This may require the development of a shared crisis protocol and information- sharing processes, in a manner consistent with human rights protections.

Respect, and for Governments protect, human rights, including by avoiding directly or indirectly contributing to adverse human rights impacts through business activities and addressing such impacts where they occur.

Recognise the important role of civil society in supporting work on the issues and commitments in the Call, including through:

- → Offering expert advice on implementing the commitments in this Call in a manner consistent with a free, open and secure internet and with international human rights law;
- → Working, including with governments and online service providers, to increase transparency;
- → Where necessary, working to support users through company appeals and complaints processes.

Affirm our willingness to continue to work together, in existing fora and relevant organisations, institutions, mechanisms and processes to assist one another and to build momentum and widen support for the Call.

Develop and support a range of practical, non-duplicative initiatives to ensure that this pledge is delivered.

Acknowledge that governments, online service providers, and civil society may wish to take further cooperative action to address a broader range of harmful online content, such as the actions that will be discussed further during the G7 Biarritz Summit, in the G20, the Aqaba Process, the Five Country Ministerial, and a range of other fora.