

Civil Society Positions on Christchurch Call Pledge

This document includes civil society, academia, and technical community perspectives regarding terrorist and violent extremist content online. The document was prepared for the Civil Society leaders' Voices for Action meeting (14 May 2019) with New Zealand Prime Minister Jacinda Ardern to discuss the Christchurch Call by an open call for input and coordination by some of those attending that meeting in Paris, France.

The document was created with input from dozens of members of civil society, including some who were in attendance on 14 May and some who were not. A non-exhaustive list of those individuals is at the bottom of this document.

Introduction

The Christchurch Call aims to address issues of “terrorism” and “violent extremism” on social media. There are a range of perspectives and voices on these issues from civil society, journalism and news media, academia, and the technical community, as well as survivors and families of victims, who care about and have valuable insight into the issues and how to minimise the harm to people, both online and offline.

This document attempts to capture some of the discussions of a range of civil society, academic, news media, and technical community members in the lead up to the Christchurch Call meetings in Paris. This document includes sections on: key issues of broad agreement, points for further discussion, process issues, and recommendations on relevant further reading.

Key Issues

In these discussions, there was **broad support for some of the key values of the Call:**

- Human rights and fundamental freedoms, including freedom of expression—to which freedom of association, religion and assembly should be added.
- A free, open, and secure Internet—to which globally connected and interoperable should be added.

There were also a range of concerns with the Call. The issues with the most shared concern were:

The **definition of “terrorism and violent extremism”** is extremely important and very problematic if left to states to individually interpret. Civic space is currently

under attack across the world—including in many established democracies. A number of democracies have leaders who are viewed by some as openly seeking to erode rule of law and dismantle institutions intended to ensure accountability and public oversight over actions that include human rights violations. It is of vital importance that governments participating in the Christchurch Call commit to robust accountability and oversight to ensure that laws, mechanisms, and other initiatives to combat terrorism online do not result in disproportionate human rights violations of political critics, human rights defenders, journalists, ethnic or religious minorities, refugees, asylum seekers, and migrants. Participating governments should also encourage other governments to do the same. There must be oversight to ensure the Call is not used as proxy legislation to legitimise such actions by governments or companies (both committing to the call and others).

The appropriate roles of tech companies and governments in taking action on these issues were robustly debated as outlined in this Call, including the specific various commitments. There is concern that the commitments made by companies and governments were based on closed-door discussions and on what these parties choose to commit to, where there are broader societal discussions about the appropriate roles of the government and the private sector on these issues, and where views differ greatly on the appropriate roles for each.

What actions are taken to address issues, and by whom, needs to be **evidence-based and with a ‘systems perspective’ on the issues**, which takes into account the systemic and complex nature of these issues, along with how “terrorism” and “violent extremism” content relate to other platform harms. We acknowledge the Call mentions the support of research and academic efforts, and the use of these to inform action is important. **Action must also be taken towards addressing these issues in our society, not just online**, including countering the underlying structural and other causes and drivers of “terrorism” and “violent extremism” by strengthening the resilience and inclusiveness of our societies. Just as technology is only part of the problem, it is also only part of the solution.

Related to this, the **process and timeline of the Call was a problem** in and of itself, including concerns about the siloed approach to negotiations and the exclusion of civil society, academic experts, journalists and news media representatives, and the technical community. We have outlined some specifics around this in an appendix to this document, focused on the process.

In the next steps around commitments of the Call, **governments and companies should engage in dialogue with each other as well as civil society, academics,**

journalists and news media, and the technical community, as well as survivors and families of victims. While the Call is an important response to a tragic moment in time, action on these issues needs to be evidence-based and carefully considered within the broader landscape of platform issues.

Technical solutions need to reflect commitments to human rights and a free, open, and secure Internet. Two specific issues that are particularly problematic in the current Call are the need to:

- Differentiate between online service providers, such as social media, and core/key infrastructure; and
- Exclude upload filters—they are inconsistent with human rights and can prevent the collection of invaluable and unique evidence of human rights abuses themselves. Once in place, such filters can be applied to other forms of expression based on historical precedent.

Below is a fuller list of points for discussion that were raised and debated. All are relevant to the Call, and address issues related to it, including more detail on the points above, as well as points with less commonly held perspective.

Points for Discussion

The following paragraphs summarise input received from various academics and civil society actors in response to the Call, and serve to synthesise key concerns and points for discussion during and after the Voices for Action meeting in Paris:

1. **Terms like “terrorism,” “terrorist content,” “online extremism,” and other related terms should be clearly defined.** The definitions of these terms vary greatly from one country and translation to the next. Even among the countries committed to the Christchurch Call, understandings of what these terms mean—and what sort of behavior and speech might be affected as governments work to implement the Call—cannot be assumed to be uniform.
2. **The scope of “online service providers,” as named in the Christchurch Call, should be limited.** Governments should not conflate social media platforms with all Internet infrastructure. Online service providers can include a broad range of services, including Internet access providers, domain name registrars, web hosts, content distribution networks, and social media platforms. Efforts to restrict content should be limited to the

level of user-generated content platforms and should not reach the infrastructure level. Broadening the scope of the Call beyond social media platforms can endanger the global and open nature of the Internet.

3. **Governments should not outsource speech regulation or governance to technology companies.** Governments should meet their own responsibilities under human rights instruments by relying upon democratically-enacted and judicially reviewable law—not proprietary terms of service. Concerns exist about the mandating of filtering technologies because of their potential negative consequences, which are not understood and cannot be addressed constructively because of the lack of transparency about them. Outsourcing speech regulation to unaccountable private actors is no more acceptable, and no more permitted under human rights law, than delegating other core functions of government.

4. **The fight against “terrorism”—both online and offline—will not succeed unless it is conducted in a manner that protects, respects, and upholds human rights.** Governments must ensure that the Christchurch Call is consistent with the UN Guiding Principles on Business and Human Rights, which stipulate that governments have a primary duty to protect human rights, while companies have a responsibility to respect human rights. Governments involved with the Call must commit to this framework and explicitly affirm that efforts to combat “violent extremism” must be consistent with human rights standards. Any such efforts will ultimately fail if they are implemented in a manner that violates human rights.

5. **The human rights risks of any new legislation or other measures should be independently assessed.** All proposed laws, administrative measures, public-private partnerships, or other initiatives that may affect freedom of expression and privacy should be subject to human rights impact assessments. Any restriction of the right to freedom of expression and opinion or the right to privacy must be prescribed by law, necessary to achieve a legitimate aim (consistent with human rights standards), and proportionate to the aim pursued.

6. **Governments should commit to robust oversight.** Any use of government power to restrict online speech, or access personal data as part of an effort to eliminate violent extremist content, must be subject to meaningful oversight against abuse of censorship or surveillance power. Without independent and credible oversight, government measures to address harmful and malicious activities via private platforms and services, or to address other social, economic, and security challenges, will be plagued by public and industry mistrust.

7. **Governments and companies alike should commit to transparency.** Governments should publish regular and accessible information and relevant data about all requirements and demands made by government entities (local, national, and regional) that result in the restriction of speech, access to information, or access to service(s). Companies should publish regular and accessible data disclosing the volume, nature, and purpose of all government requests made to companies affecting users' freedom of expression and privacy.

8. **Governments and companies should ensure that people have access to adequate remedy.** People have a right to meaningful and effective remedy, including legal recourse, when their privacy or freedom of expression rights are violated. Just as companies should implement private remedy mechanisms, governments must commit to ensure that individuals have a clear right to legal action when their human rights and civil liberties are violated by any government authority, corporate entity, or company complying with a government demand.

9. **Governments, civil society, journalists and news media, and the private sector should collaborate to prevent their responses to alleged platform harms from infringing human rights.** Governments that are committed to protecting freedom of expression online should commit to work proactively and collaboratively with one another, as well as with civil society, journalists and news media, and the private sector, to establish a positive roadmap for addressing online harms without causing collateral infringement of human rights. New Zealand and France are both members of the Freedom Online Coalition, as are other governments such as Canada that will be participating in the Christchurch Call. Governments should commit to

ensure that efforts to combat “violent extremism” online are coordinated and consistent with their commitments and multilateral efforts to promote a free, globally connected, and open Internet.

10. **Governments should commit to supporting freedom of expression globally.** Violent social movements are more likely to proliferate and thrive unchallenged in communities that lack credible and vibrant independent media and spaces for public discourse, including those that are designed for public interest purposes and not primarily the maximisation of advertising revenue. Domestic and foreign policies, including trade, development, and economic policies, should support the flourishing of diverse information ecosystems where people have the ability to choose among alternative platforms for online discourse.
11. **Politicians and government actors must not encourage or condone violent ideologies.** State actors rarely face the same consequences for their speech as do ordinary citizens. Politicians and other government actors bear special responsibilities and must be accountable for using such language, both online and offline, that incites violence, hatred, or discrimination.
12. **Internet shutdowns and the temporary blocking of websites by governments and Internet service providers (ISPs) should be avoided.** Any actions taken to prevent the spread of terrorist content should be targeted, specific, and proportionate. Blocking access to the Internet, in whole or in part, can have unintended consequences for freedom of expression, access to information, economies, sustainable development, and safety.
13. **Upload filters and rapid erasing of content can be counterproductive to understanding and taking action against “terrorism” and “violent extremism.”** Content on social media provides an invaluable and unique trove of evidence of human rights abuses committed by extremist groups and by governments. The International Criminal Court and prosecutors in the European Union have relied on such evidence to conduct investigations and bring charges, and human rights investigators seek out this material and create archives of verified content that will be essential in future justice

processes. When platforms immediately delete this content as it appears without reaching out to investigators, however, opportunities to address the root causes of extremism are also deleted. “Counter speech,” journalistic reporting, and other protected speech is vital to countering extremism. Filters and censorship can limit the ability of civil society, academics, and law enforcement to understand the tactics and arguments of extremists.

14. **The automated removal of “extremist content” cannot currently be done in a rights-respecting way.** Technology platforms are already using opaque artificial intelligence processes known as machine learning algorithms to find so-called extremist content, and these algorithms have already deleted hundreds of thousands of videos improperly. They rely on an initial set of training data that may exhibit cultural and linguistic bias, but then they teach themselves. Unless they are specifically designed to be understandable, and made available to review for those outside of corporations, even their creators cannot understand why they make the decisions they make—leaving no room for transparency, accountability, or redress mechanisms. The call should therefore explicitly reject unaccountable removal of content, and eliminate incentives for over-removal of content.

Process Issues with Christchurch Call

Civil society participation in the Christchurch Call process has been impacted by various factors:

1. Negotiating the Christchurch Call among the governments and tech corporations without including civil society from the beginning.
2. Civil society and the technical community was informed about this process at a very late stage.
3. The pledge text was not made public, and only invitees received the text (and belatedly).
4. Resistance to include civil society from some governments.

5. Closed and non-transparent meetings that are only informational for civil society
6. Not including civil society in the finalisation of the pledge text.
7. Not including individuals and groups (such as Muslims, organisations in the Global South and in countries deeply affected by terrorism, and people/groups who are the targets and victims of bigoted violence), as well as those groups who are censored under similar frameworks.
8. Short-circuiting civil society consultation and holding this meeting during Ramadan.

Civil Society Participation in future processes (beyond Voices for Action)

The Christchurch Call acknowledges 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, the G20, the Aqaba process, the Five Country Ministerial, and a range of other fora.”** Considering the procedural shortcomings in including civil society voices in multilateral fora, civil society participation in the future processes will be mainly dependent on overcoming the current procedural barriers, i.e. not holding the processes in a multilateral setting.

Suggestions for taking the discussion forward (after the Paris meetings) at relevant Internet policy and governance arenas:

1. Participate at relevant events and in relevant processes like the Internet Governance Forum (IGF), RightsCon Summit Series, the UN Secretary-General’s High-Level Panel on Digital Cooperation (HLPDC), the Stockholm Internet Forum, the Freedom Online Coalition’s Annual Meeting(s) and Advisory Network meetings, various national and regional IGF meetings, country-level consultations on online harms (e.g. France and the UK’s online harms/platform duties proposals), and other relevant events.
2. As far as is reasonably possible, consult with a broad range of stakeholders and interested parties, including those not typically active in Internet governance and digital policy arenas, including human rights groups, anti-racism organisations, refugee councils, development communities, etc.
3. To enable better and broader public participation, the text of the Call should be published online on a review platform (e.g., NetMundial style) to enable any relevant stakeholders to comment on and provide input on the Call and its practical implementation.

4. Provision should be made to support, commission, and fund rigorous research into rights-respecting ways of limiting terrorism and violent extremism on social media, and to understanding the impact of related harms within a broader context of platform responsibility and/or harms. This should include a comprehensive assessment of measures set out in existing laws, including initiatives at all levels: the EU Counter-terrorism directive, Additional Protocol to the Council of Europe's Convention on the Prevention of Terrorism or UN Security resolution 2178 etc.

Further Reading

Before setting new precedents, we would recommend identifying and reviewing existing declarations, principles, recommendations, laws and by-laws that define and regulate this space and propose checks and balances that hold actors accountable for the impact that their work has on freedom of expression and human rights.

Fundamental Principles

The Manila Principles on Intermediary Liability (2015).

<https://www.manilaprinciples.org/>

The Tshwane Principles on National Security and the Right to Information (2013).

<https://www.opensocietyfoundations.org/sites/default/files/tshwane-principles-15-points-09182013.pdf>

The UN Guiding Principles on Business and Human Rights (2011).

<https://www.business-humanrights.org/en/un-guiding-principles>

The Johannesburg Principles on National Security, Freedom of Expression and Access to Information (1996).

<https://www.article19.org/wp-content/uploads/2018/02/joburg-principles.pdf>

Global Network Initiative Principles on Free Expression and Privacy (updated 2017).

<https://globalnetworkinitiative.org/gni-principles/>

Responses to the European Commission's Terrorism Regulation

The European Commission's proposed terrorism regulation raises similar concerns to those expressed above. The following documents, while pertaining specifically to the EC regulation, offer clear recommendations on how to ensure the protection of human rights.

European Digital Rights Initiative (EDRi)'s document pool on the terrorism regulation, <https://edri.org/terrorist-content-regulation-document-pool/>.

WITNESS-led letter focused on global effect and evidentiary value
https://drive.google.com/file/d/1WTgl5hjJ_cAE1U0OjqaQ9AucU6HNIhoi/view

Joint civil society letter regarding the hashing database used by major Silicon Valley companies,
<https://edri.org/files/counterterrorism/20190205-Civil-Society-Letter-to-EP-Terrorism-Database.pdf>

CDT-led civil society letter on the proposed regulation,
<https://cdt.org/insight/letter-to-ministers-of-justice-and-home-affairs-on-the-proposed-regulation-on-terrorist-content-online/>

Joint Letter of the UN Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2018),
<https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=24234>

Global Network Initiative statement on the proposed regulation (2019).
<https://globalnetworkinitiative.org/wp-content/uploads/2019/01/GNI-Statement-Proposed-EU-Regulation-on-Terrorist-Content.pdf>

Comprehensive literature review on online content restrictions

A comprehensive 2017 literature review, conducted by London's International Centre for the Study of Radicalisation, found that only a minority of published research supported "hard" approaches such as "the restriction of Internet content for security purposes," and that "[m]ost work on this topic regards such measures as impractical at best and dangerous at worst."

Alexander Meleagrou-Hitchens and Nick Kaderbhai, International Centre for the Study of Radicalisation, King's College London, Research Perspectives on Radicalization: A Literature Review, 2006-2016 (2017), 53, 56.

Neumann, Peter R., Options and Strategies for Countering Online Radicalization in the United States, Studies in Conflict & Terrorism (January 2013) 431-459 at 437.

J.M. Berger and Jonathon Morgan, The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter, Brookings Project on U.S. Relations with the Islamic World Analysis Paper No. 20 (March 2015), 54.

Ines von Behr, Anaïs Reding, Charlie Edwards, and Luke Gribbon, Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism, Rand Europe (2013).

Other recommendations

Council of Europe, Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (2018).

https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2018).

<https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>

Global Network Initiative, “Policy Brief: Extremist Content and the ICT Sector,” November 2016.

<https://globalnetworkinitiative.org/wp-content/uploads/2016/12/Extremist-Content-and-ICT-Sector.pdf>

OHCHR, “Comments on legislation and policy,”

<https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/LegislationAndPolicy.aspx>

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2010).

<https://www2.ohchr.org/english/bodies/hrcouncil/docs/16session/a-hrc-16-51.pdf>

Michelle Bachelet, “‘Smart mix’ of measures needed to regulate new technologies” (2019).

<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24509&LangID=E>

Other resources and links

Dr. Courtney Radsch, “Media Development and Countering Violent Extremism: An Uneasy Relationship, a Need for Dialogue,” Center for International Media Assistance (CIMA), October 2016.

https://www.cima.ned.org/wp-content/uploads/2016/10/CIMA-CVE-Paper_web-150ppi.pdf

Dr. Kate Ferguson, “Countering violent extremism through media and communication strategies: A review of the evidence,” Partnership for Conflict, Crime, & Security Research, March 2016.

<http://www.paccsresearch.org.uk/wp-content/uploads/2016/03/Countering-Violent-Extremism-Through-Media-and-Communication-Strategies-.pdf>

Global Forum for Media Development, “Governing Digital Convergence: An Issue Paper on Media Development and Internet Governance,” November 2018.

https://docs.google.com/document/d/1hMclf0hz2PXa_VhO17w2iRhFpvi-NZ0yeY2mJCN6QBA/edit

Global Partners Digital, “A Rights-Respecting Model of Online Content Regulation by Platforms,” May

2018. <https://www.gp-digital.org/wp-content/uploads/2018/05/A-rights-respecting-model-of-online-content-regulation-by-platforms.pdf>

Organisation for Security and Co-Operation in Europe (OSCE), Charter on Preventing and Combating Terrorism (2002). <https://www.osce.org/odihr/16609>

UNESCO, “Preventing Violent Extremism.

<https://en.unesco.org/preventing-violent-extremism>

Authors

The following is a non-exhaustive list of contributors to this document. Additional input was provided by anonymous contributors and during calls leading up to the meetings.

- Farzaneh Badii (Internet Governance Project, Georgia Tech)
- Ben Decker (Disinformation Index)
- Anriette Esterhuysen (Global Commission on Internet Governance)
- Claire Fernandez (European Digital Rights Initiative)
- Gabrielle Guillemin (Article 19)
- Dia Kayyali (Witness)
- Daphne Keller (Center for Internet and Society, Stanford University)

- Gayatri Khandhadai (Association for Progressive Communications)
- Cheryl Leanza (A Learned Hand)
- Rebecca MacKinnon (Ranking Digital Rights)
- Mira Milosevic (Global Forum for Media Development)
- Milton Mueller (Internet Governance Project, Georgia Tech)
- Michael Oghia (Global Forum for Media Development)
- Julie Owono (Internet Sans Frontieres)
- Javier Pallero (Access Now)
- Jason Pielemeier (Global Network Initiative)
- Courtney Radsch (Committee to Protect Journalists)
- Ellen Strickland (InternetNZ)
- Anri van der Spuy (Research ICT Africa)
- Deirdre Williams
- Jillian C. York (Electronic Frontier Foundation)