

Christchurch Call Community Consultation

FINAL REPORT

Joint Foreword

President Emmanuel Macron and Prime Minister Jacinda Ardern

CHRISTCHURCH CALL COMMUNITY CONSULTATION REPORT.





The misuse of the internet to promote terrorism and violent extremism is an issue that transcends borders. It reaches into our social networks, our communities, and our families, and has real impacts in the offline world.

When a terrorist opened fire in two mosques in Christchurch, New Zealand, in March 2019, 51 Muslim worshippers lost their lives. Dozens more were seriously injured.

The attack was livestreamed in an attempt to subvert the technology platforms we use to connect to instead push messages of hate and extremist ideology.

Left unchecked, this kind of abuse of the internet risks inciting more real world terrorist acts.

Supporters of the Christchurch Call to Action, alongside supporters of other international initiatives such as the G20, the G7, and the Aqaba Process established by the Hashemite Kingdom of Jordan, are focused on a common principle: there is no place for terrorist and violent extremist content online.

The results in this report, our first community-wide stocktake, tell us the Christchurch Call is making a tangible difference.

We are proud of the real progress we have achieved together already, across many of the Call's commitments.

Collectively, we have three protocols for responding quickly to crisis incidents; tech companies have reformed the Global Internet Forum to Counter Terrorism into an independent entity and its multi-stakeholder work is under way; governments, companies and civil society groups are working together in new ways; and an increased focus on research into terrorism and violent extremist content online provides a strong base to develop further work.

It is heartening to see, detailed in the report, the wide range of other initiatives supporters have undertaken as part of the Call in their countries and companies.

The development of the Christchurch Call Advisory Network has also provided opportunities for deeper, more structured engagement with civil society, built on the shared understanding that a free, open and secure internet is a powerful tool to promote connectivity, enhance social inclusion and foster economic growth.

With the foundations we have laid, as described in this report, we can now look to refine our focus and redouble our efforts.

The many attacks since Christchurch – including in Colombo, El Paso, Dayton, Halle, Glendale, Nakhon Ratchasima, Conflans-Saint Honorine, Nice and Vienna – bear witness to the challenge we face.

We must continue to work towards better understanding the algorithms that promote content online, to identify intervention points and prevent exploitation by malicious actors.

We must also ensure that we take a consistent view of terrorist and violent extremist content – one that accounts for a range of media, whether still images or live broadcasts, and that addresses content propagated outside a live emergency response.

And we must continue to work together, each taking responsibility for the part that we can play in pursuit of the enduring goal of the Christchurch Call to Action, to eliminate terrorist and violent extremist content online.

Right Honourable Jacinda ArdernPrime Minister of New Zealand

His Excellency Emmanuel Macron President of the French Republic

Executive Summary

On 15 March 2019, a terrorist livestreamed an attack on two mosques in Christchurch, New Zealand. 51 people were killed and 50 injured. Including views during the live broadcast, the original video was seen some 4,000 times before it was removed from Facebook. Copies of the terrorist's video continue to be uploaded online, and have been seen millions of times on the internet.

Two months later in Paris on 15 May 2019. Prime Minister Jacinda Ardern and President Emmanuel Macron launched the Christchurch Call (the Call) to eliminate Terrorist and Violent Extremist Content (TVEC) online. The Call is a set of voluntary commitments by supporters - governments and companies - based on the conviction that a free, open, and secure internet offers extraordinary benefits to society. Respect for human rights law and fundamental freedoms, includina freedom of expression, underpins the approach in the Call. The Call also reflects the importance of a multistakeholder commitment to ensuring TVEC is not shared online.

A year and a half later, the governments of New Zealand and France – as cofounders of the Call – conducted The Christchurch Call Community Consultation to better understand how Call supporters have implemented the Call's commitments, and to identify those areas in which further work is needed. Responses were sought from all government and industry supporters of the Call, as well as from members of

the Christchurch Call Advisory Network (CCAN). The consultation was open to submissions from 21 September to 30 October 2020. In total, members of the Call community submitted 39 responses.

This report summarises the contributions received, and presents key findings from the consultation. Its purpose is to provide a snapshot of the measures implemented by supporters to meet Call commitments, to understand their perceptions of the initiative's effectiveness, and to assist in identifying productive areas for further work.

The analysis of the consultation data was conducted by officials from the French and New Zealand governments. The original contributions have been released in an open format on the <u>Christchurch Call website 1</u>.

¹_https://www.christchurchcall.com/

What are the main achievements of the Christchurch Call since May 15th, 2019?

In less than two years, the Call's stakeholders – governments, technology companies, and civil society representatives – indicate they have made major progress in four areas:

- Increasing international awareness on the importance of tackling TVEC online;
- Promoting multistakeholder collaboration against TVEC online;
- Reforming the Global Internet Forum to Counter Terrorism (GIFCT); and
- Developing crisis protocols to limit the virality of TVEC online in the case of real-world attacks

These achievements align well with the purposes of the Call, demonstrating the strength of its guiding principles and multistakeholder approach.

How effective has the Christchurch Call been so far?

Overall, a majority of respondents describe the Call's impact as "good"

or "very good". The results also indicate additional work is needed – in collaboration with civil society organizations – to foster greater multistakeholder cooperation on the issue.

How have supporters implemented their commitments so far?

The Community Consultation enabled Call supporters to share the steps they have taken since 15 May 2019 to counter TVEC online. Government respondents state they have taken action to strengthen resilience and inclusion in their societies, and to ensure effective enforcement of applicable laws that prohibit the production or dissemination of TVEC. All respondent companies report taking specific measures to prevent the upload, livestream, and dissemination of TVEC on their services, while providing regular and transparent public reporting on the quantity and nature of TVEC detected and removed.

Overall, significant steps have been taken at both national and industry levels, demonstrating progress towards delivering on the ambition of the Call. Further collaboration and information sharing is expected to enhance the implementation of our common goals.

What should the next steps be for the Christchurch Call?

The Community Consultation respondents suggested a range of ambitious improvements to the implementation of the Call, including:

- Promoting better collaboration between companies and national authorities, especially in times of crisis;
- Increasing the number of companies supporting the Call;
- Increasing dialogue between stakeholder groups;
- Advancing a definitive understanding of TVEC online;
- Improving transparency measures implemented by Call supporting companies;

- Fostering a common understanding of relevant legal frameworks;
- Assessing the role of algorithms in promoting TVEC, to support the development of effective, positive interventions; and
- Taking action against the drivers of terrorism and violent extremism, including addressing content that incites and/or glorifies terrorist and violent extremist acts.

In addition, New Zealand and France have identified key questions from the answers provided during the Community Consultation by governments, online service providers, and civil society, for consideration by the Call community:

I/ GOVERNMENT COMMITMENTS

Countering Terrorist and Violent Extremist Content by Building Resilient and Inclusive Societies

 Can best practices be shared across governments to ensure that relevant media campaigns and educational initiatives effectively reach our population, including vulnerable communities?

Legal Measures to Address Terrorist and Violent Extremist Content

 While ensuring privacy and innovation, satisfying the requirements of all stakeholders, and remaining conscious of existing legal frameworks – what challenges and opportunities can be identified in the sharing of information and data related to the moderation of TVEC online?

Media Standards and Frameworks

 What qualities of successful media standards and frameworks have been the most effective in managing instances of TVEC being amplified by the media?

Preventing Exploitation of Online Services for the Dissemination of Terrorist and Violent Extremist Content

 How can we best support the exchange of information on regulatory measures, industry standards and voluntary frameworks, and awareness-raising/capacity-building activities established within each supporting country?

Other

How can we ensure the momentum of the Call continues in its third year?

II/ ONLINE SERVICE PROVIDERS COMMITMENTS

Prevention of Terrorist and Violent Extremist Content Online

 What can we learn from recent efforts of supporting companies to further develop transparent measures preventing the upload of TVEC, including its immediate and permanent removal, without prejudice to law enforcement and user appeals requirements? How can these efforts be supported by governments and civil society?

Transparency and Enforcement of Community Standards and Terms of Service

 Are there opportunities for supporting companies to work more closely with civil society organizations, including the CCAN, in the development and implementation of community standards and terms of service, with particular regard to redress and complaints mechanisms?

Reporting on Terrorist and Violent Extremist Content Detection and Removal

 How can supporting companies continue to improve on their commitments towards meaningful transparency in their reporting, and how can this be supported by governments and civil society?

Algorithmic Processes

- How can supporting companies working with governments, academia, and civil society
 provide more transparent insights into the function of recommendation algorithms,
 including where these may have unintended or harmful consequences?
- How can supporters work together on the development and delivery of "positive intervention" mechanisms to counter TVEC?

Other

 How can we best build a shared understanding among the multistakeholder community on the GIFCT's work, on how it is best able to deliver on its mission, and on how to enable the widest possible multistakeholder engagement in that work?

III/ JOINT COMMITMENTS FOR COUNTRY AND COMPANY SUPPORTERS

Engagement with Civil Society

 How can we improve engagement with civil society, and how can we encourage participation from organisations across a wide range of geographies?

Information Sharing and Algorithmic Processes

- To what extent does countering the spread of TVEC online require modifications in the design of recommendation algorithms used by online platforms?
- How can we ensure the GIFCT's Content-Sharing Algorithms, Processes, and Positive Interventions (CAPPI) Working Group makes good progress based on trusted information sharing? How do we ensure the group's work is incorporated into the policy-making of companies?

Technical Solutions

 How can Call supporters improve the research and development of technical solutions to prevent the upload of TVEC online, and enable its detection and immediate removal? How can that work best be shared through open channels to the wider community?

Research

How can governments and companies better facilitate research into technical solutions?
 How can they further their support of research and academic efforts to better understand, prevent, and counter TVEC online?

Cooperation with Law Enforcement Agencies

• In the event of an online crisis, how can government agencies better administer outreach to companies to ensure communication with the tech sector is consistent and clear, and that lawful requirements of law enforcement agencies are met?

Additional Question for Company Supporters Only: Support for Smaller Platforms

- How might smaller Call supporting companies be better supported?
- What unique insights can smaller tech companies bring to Call supporting companies in the global effort to eliminate TVEC online?

International Cooperation and Collaborative Actions Taken

- How can we ensure the Call's multistakeholder collaboration approach continues to develop in the long term? How can we ensure this approach secures support from a broader range of actors from the tech industry?
- What can be done to support partner countries, including those with limited capacity, in implementing the commitments of the Call?

Crisis Response

- How can the different crisis protocol frameworks be enhanced to ensure a holistic, well understood, and collaborative approach to online crisis management, which meets the needs of all stakeholders?
- Are there further creative opportunities for workshops focused on the operational multistakeholder response to a real life terrorist and violent extremist event with an online component?

Protection of, and Respect for Human Rights

 How can Call supporters assist each other in ensuring implementation is consistent with respect for international human rights law, fundamental freedoms, and a free, open, and secure internet? How might the Call be more active in this?

Table of Contents

TABLE OF CONTENTS

l.	Introduction		10
II.	Methodology		14
III.	l. Responses		16
IV.	V. How have Christchurch Call supporters upheld their		
	commitments?		17
	1.	Government Commitments	17
	2.	Online Service Providers Commitments	30
	3.	Joint Commitments for country and company supporters	40
IV.	IV. Progress and next steps		
	1.	Achievements of the Christchurch Call	62
	2.	How effective has the Christchurch Call been so far?	65
	3.	Next steps for the Christchurch Call	66
ıv	Conclusion		69

I. Introduction

On 15 March 2019, a gunman opened fire on Muslim worshippers at the Al Noor and Linwood mosques in Christchurch, New Zealand. In a racially and ideologically motivated attack, the Christchurch terrorist murdered 51 people and injured 50 more. The perpetrator livestreamed his atrocities on Facebook. The video was designed to go viral.

In the hours, weeks, and months after the attack, the video and thousands of replicas were viewed countless times – often inadvertently – as malicious actors sought to manipulate the algorithms that boost online content. In the 24 hours following the attack, a copy of the video was uploaded to YouTube every second. Facebook removed more than 4.5 million videos and photos of the attack in the months following.

Extensive efforts by the technology companies to remove the footage from their platforms were frustrated by the deliberate and relentless modification of the footage to avoid the existing content moderation tools. It remains available in corners of the internet, despite ongoing action to remove it.

The online impact of the Christchurch terrorist attack was an order of magnitude larger than anything we had seen before on the internet.

THE CHRISTCHURCH CALL TO ACTION RESULTED FROM THAT ABHORRENT ACT.

On 15 May 2019, two months to the day after the attack, New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron convened a group of government and technology sector leaders to launch the Call to eliminate TVEC online.

The <u>Call</u>² is a series of voluntary commitments made by supporting governments and technology companies. It rests on the shared understanding that elimination of TVEC online should be conducted in a manner consistent with international human rights law and fundamental freedoms, including freedom of expression. The Call champions a free, open, and secure internet as a global good.

The Call recognizes TVEC online as an abhorrent problem – one that is beyond the capacity of either governments or industry to solve alone.

Our best chance lies with governments and industry working together. The Call's text therefore includes individual and joint commitments for these participants. It also recognizes the vital role of civil society supporting these efforts, including the promotion of full respect for human rights and fundamental freedoms in this work.

The Call community now comprises 48 countries, two international organizations, the European Commission, and 10 technology companies. The CCAN, comprised of 44 international academic and non-governmental organisations, provides valuable advice to supporters.

COMMITMENTS

Our strongest defence against terrorism and violent extremism is a cohesive and resilient society. Call commitments therefore focus on both prevention and response.

Elements of prevention include:

- Direct actions to strengthen the resilience and inclusiveness of our societies;
- Research to increase our understanding of TVEC online;
- Building media literacy to counter distorted terrorist and violent extremist narratives;
- Encouraging responsible reporting of terrorist events; and
- International collaboration to counter terrorism and violent extremism in all its forms.

Effective responses to serious TVEC online incidents are vital to reduce the harms associated with this content. Aspects of response include:

- Effective crisis response protocols;
- Enforcement of terms of service and community standards;
- Enforcement of fit-for-purpose legislation;
- Ensuring algorithmic outcomes do not expose more people to TVEC; and
- Effective communication between companies and governments during a crisis.

DEVELOPMENTS

The Call community welcomed the reform of the GIFCT as an independent organization supported by its founding company members in 2020. This organisation is well placed to take forward work on several Call priorities, including through its multistakeholder working groups.

Sadly, there have been numerous terrorist and violent extremist incidents since the launch of the Call, many with an online component. Attacks in Halle, Germany and Glendale, Arizona triggered the GIFCT's CIP – a collaborative technical solution for industry, which did not exist at the time of the Christchurch attacks – that enables the swift removal of perpetrator-generated TVEC across online platforms. A range of complementary domestic and regional protocols have subsequently emerged, including the Call's own Crisis Response Protocol to facilitate crisis communication between governments and industry.

More recently, the terrorist attacks in Conflans-Sainte-Honorine, Nice, and Vienna, have underlined the evolving nature of TVEC online. A particularly concerning aspect of the attack in Conflans-Sainte-Honorine was the speed with which violent extremist content incited the murder of school teacher Samuel Paty. In the face of these developments, the Call community must remain accountable to the commitments to which we have collectively agreed, and responsive to the evolving threat of terrorism and violent extremism online.

THE REPORT

This report illustrates the breadth and depth of work already underway across the community of Call supporters. It is encouraging to see what has been achieved in eighteen months, and we welcome the complementary efforts described in this report. The report also identifies areas where further work is required. These include further refinement of crisis response, transparency reporting, measures to address the full scope of content considered "TVEC", and broader social cohesion measures.

We extend our sincere thanks to the Call supporters and CCAN members who provided responses. We acknowledge the strain placed on all supporters by the COVID-19 pandemic, and the challenges some faced in responding to this exercise. This is the first iteration of what we hope will become a regular exercise, and over time, more representative of the wider Call's network of supporters.

We hope this report and the consultation data will be a valuable resource to both supporters and others, and that it will promote discussion, action, and further progress against a challenge that threatens the peace and security of all.

Eliminating TVEC online is not something that can be addressed wholly within the confines of one country's policies, rules, and regulations. Call supporters must continue to collaboratively, and independently demonstrate substantial delivery on Call commitments.

He waka eke noa.

Nous sommes tous concernés.

We are all in this together.

II. Methodology

In the spirit of the multistakeholder model of the Call, New Zealand and France worked alongside the CCAN to draft a questionnaire for supporting governments and companies, aligned with the commitments of the Call. Following consultation with representatives of the CCAN, a section comprising additional questions was developed to enable CCAN members to contribute their perspectives on the Call, including on its efficacy as a multistakeholder initiative.

Responses to this questionnaire were sought from the companies and governments that had formally expressed support for the Call on or before 23 September 2019, on the basis that this group had established and developed initiatives to meet voluntary commitments under the Call. Looking forward, we are eager to hear how newer supporters, and those otherwise unable to contribute to this exercise, have developed their efforts.

STRUCTURE OF THE CONSULTATION

The questions were structured with two objectives: to cast a wide net - capturing as many responses from the Call community as possible - and to create a format that would stimulate a wide range of perspectives. We utilised a combination of both open and closed format questions to achieve these objectives.

The closed format questions were the core sections of the questionnaire, and were directly related to the voluntary commitments of the Call. For the open format questions, four and five point Likert scales were used to seek comment beyond a [YES] or [NO] response. These open format questions offered respondents an opportunity to provide insights into supporters' perceptions of the Call's efficacy in the 18 months since its launch. This includes commentary on accomplishments to date, and areas where further work is needed or where future attention might be best directed, both independently and collectively, by supporters.

The Community Consultation was not envisaged to function as a "transparency report" for Call supporters. Rather, we sought to establish a "baseline" of progress, and to inform the direction of future efforts.

New Zealand and France were cognisant during the consultation of the impact of COVID-19 on the availability of supporters' resources, and capacity

to undertake an extensive multistakeholder exercise. With this in mind, a 500 character limit was set for responses.

Some respondents contributed responses in excess of the 500 character limit, in separate documents. In the majority of cases, this was because further context was considered necessary to support an initial contribution. Consistent with the instructions provided with the questionnaire, the information used to inform this report and direct citations have been limited to the first 500 characters. Full submissions will be hosted on the Call's website, alongside information registered via the online survey software Typeform. Citations in this report from responses over 500 characters in length will be marked with an acknowledgement (*) that further content was provided, and is available to read online.

The final version of the questionnaire contained a total of 40 questions.

- Section 1A: Government commitments (six questions)
- Section 1B: Online service provider commitments (six questions)
- Section 2A. Joint commitments [governments only] (nine questions)
- Section 2B: Joint commitments [companies only] (10 questions)
- Section 3: Current and future perspectives [same questions for governments, companies and civil society] (five questions); and
- Section 4: About you [same questions for governments, companies and civil society] (four questions).

Supporters were advised that organisation names would be included in reporting, unless the respondent expressly objected. Personally identifiable information provided would be omitted.

A preliminary, quantitative report on the inaugural Christchurch Call Community Consultation exercise was published on the <u>Christchurch Call's website</u>³ to accompany a Call session at the 2020 Paris Peace Forum.

The Paris Peace Forum session "<u>Christchurch Call: Defining the Next Steps</u> Collectively" can be found on the Forum's YouTube channel ⁴.

³ https://www.christchurchcall.com

⁴Paris Peace Forum: https://www.youtube.com/channel/UCxGMAzbzv77Jk8otRyhsUag

III. Respondents

In total, we received 39 individual contributions. Six of the seven companies that supported the Call as at September 2019 submitted contributions. Roughly half of the Call supporting governments and international organizations submitted contributions. New Zealand and France are grateful for the contributions of several members of the CCAN.

The following Call supporters submitted contributions:

- Governments and institutions (24 out of 48 Call supporters):
 Australia, Belgium, Canada, Colombia, Cyprus, Denmark, the
 European Commission, Finland, France, Georgia⁵, Germany,
 Hungary, Iceland, India, Ireland, Italy, Japan, Latvia, Malta, New
 Zealand, Portugal, Romania, Sweden, United Kingdom;
- Online service providers (six out of seven Call supporters): Amazon (Twitch), Dailymotion, Facebook, Google/YouTube, Microsoft, Twitter;
- Members of the CCAN (nine out of 44): Center for Democracy & Technology, GDI, Global Forum for Media Development (GFMD), InternetNZ, Institute for Strategic Dialogue (ISD), Islamic Women's Council of New Zealand, Mnemonic (Syrian Archive), New America's Open Technology Institute, Women's Organisation of the Waikato Muslim Association (WOWMA).

Stakeholders were asked for their level of knowledge of work under the Call. Of 35 stakeholders who answered, most have a "good" or "very good" knowledge (58%). More than three quarters of the companies stated having a "very good" knowledge of work under the umbrella of the Call.

A relatively small portion of the stakeholders (31%), consider their understanding of Call work as "average". Two governments believe they do not have a good knowledge of the initiative. Only one company considers its understanding as "average". These responses suggest a need to devise more effective practices for keeping the Call's community informed and engaged going forward.

⁵ Georgia's contribution arrived after the publication of the preliminary report, and was not included in the initial statistical analysis.

IV. How have Christchurch Call supporters upheld their commitments?

GOVERNMENT COMMITMENTS

In supporting the Call, government supporters have agreed to a number of voluntary commitments, including:

- To counter the drivers of terrorism and violent extremism by strengthening the resilience and inclusiveness of our societies;
- To ensure effective enforcement of applicable laws that prohibit the production or dissemination of TVEC;
- To encourage media outlets to apply ethical standards when depicting terrorist events online;
- To support frameworks such as industry standards to ensure reporting on terrorist attacks does not amplify TVEC; and
- To consider appropriate action to prevent the use of online services to disseminate TVEC.

First Question for Government Supporters: Countering Terrorist and Violent Extremist Content by Building Resilient and Inclusive Societies

"Since supporting the Christchurch Call, has your government taken action to counter the drivers of terrorism and violent extremism by strengthening the resilience and inclusiveness of your society to resist terrorist and violent extremist ideologies? (For example through education; media literacy; and the fight against inequality)" Relevant Commitment: To counter the drivers of terrorism and violent extremism by 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.

This commitment acknowledges that our response to the issue of TVEC online must address both online and offline factors. It encourages governments to take a holistic approach to tackling TVEC online, including by increasing the capacity of their citizens to both recognise and resist TVEC online. The vast majority of participating governments (21/24) report having taken action in this area.

Some governments have been guided in their efforts by overarching strategies or plans; others have taken a targeted approach to address specific concerns (e.g. racism or hate speech). Some also reported the addition of significant new funding to community resilience initiatives (e.g. <u>Canada's CAD 45 million investment in a strategy to combat racism</u> ⁶, and the European Commission's earmarking of EUR 30 million over three years to support its <u>Radicalisation Awareness Network</u> ⁷).

Looking at the data in more detail, the actions can be grouped into five categories:

Development of national strategies or plans – several respondents provided details of strategies that were either new or significantly enhanced after the founding of the Call. These included: France's National Action Plan on Preventing Radicalisation⁸, the Irish Government's Action Plan for Online Safety⁹, and elements of Portugal's National Strategy to Counter Terrorism ¹⁰ (protect, pursue and respond pillars). Colombia detailed two separate but complementary strategies: one attempting to provide a "whole of government response" to prevention, and one dealing with the acts of terrorism and violent extremism within the context of law enforcement.

⁶https://www.canada.ca/en/canadian-heritage/news/2020/12/building-a-more-inclusive-canada-the-government-of-canada-supports-anti-racism-projects-in-yukon.html

⁷ https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation awareness network en

⁸ http://www.gouvernement.fr/radicalisation-les-cinq-grands-axes-du-plan-prevenir-pour-proteger

⁹ https://www.gov.ie/en/publication/77f39d-action-plan-for-online-safety-2018-2019/

¹⁰ https://dre.pt/application/conteudo/66567251

"The Colombian State has an anti-terrorist strategy with various elements that in a transversal way link up all the institutions in charge of dealing with prevention, protection and prosecution of this calamity. Regarding the specifics of violent radicalization, violent extremism and its relation with the crime of terrorism, Colombia has developed a National Strategy. Also, the Office of the Attorney General includes the Commissioner against Organized Crime, two groups of prosecutors specialized in the area, as well as criminal analysts and the judiciary police with expertise in these criminal trends."

Colombia (translation) (*)

Cross sectoral initiatives - these include programmes where the services of multiple front-line providers are coordinated to provide assessment and support to people at risk of radicalisation, such as the UK's 'Prevent' programme 11, and Malta's 'Prevent Network'. The Swedish Centre for Preventing Violent Extremism¹² was established on 1 January 2020, with the aim of developing evidence based and cross-sectoral work, to prevent violent extremism at all levels of the governance (national, regional and local).

Harnessing the power of civil society and industry - several countries reported multistakeholder initiatives, Japan's "public-private study groups" that bring together government agencies and industry to raise awareness of international efforts to prevent TVEC online, and Ireland's Action Plan for Online Safety¹³ , which mandates collaboration between government, industry, families, and the EU. In Denmark, the Security and Intelligence Service, along with Government agencies, work directly with civil society groups to develop programmes that deliver a strong "social cohesion" element.

¹¹ https://www.gov.uk/government/publications/prevent-duty-guidance

¹² https://www.cve.se/om-cve/in-english.html

¹⁹https://www.gov.ie/en/publication/77f39d-action-plan-for-online-safety-2018-2019/

"A 'National Alliance against Online Radicalisation', established by Denmark's Security Intelligence Service brings together government agencies and civil society in a shared value community to mobilise civil society to develop CVE initiatives. Supported projects are designed to increase digital literacy; strengthen the role of peers and families; increase teachers' knowledge and awareness; and support civil society organisation."

Denmark

Media campaigns and initiatives – many government supporters report action in this area. Australia has employed a blend of communication and community activities to counter terrorist and violent extremist propaganda, and strengthen social cohesion. This includes articulation of an inclusive national identity on social media, and messages to build trust within the Australian community. Malta has sponsored positive campaigns to promote resilient and inclusive societies. Other respondents report media campaigns targeted at specific issues: New Zealand's 'Give Nothing to Racism' campaign¹⁴, Italy's promotion of tolerance via traditional media sources¹⁵, and Sweden's 'No Hate Speech' campaign. ¹⁶

Education initiatives – digital literacy is a common focus of education initiatives, as demonstrated in Belgium, Canada, Germany, and the UK (the latter is working on an Online Media Literacy Strategy ¹⁷).

Canada's Digital Citizen Initiative¹⁸ provides funding to promote digital literacy and evidencebased policy. Other education initiatives include Germany's civic education work (designed to foster democratic awareness and encourage participation in the political process), and France's Interministerial Committee for Preventing Delinquency and Radicalisation¹⁹, which seeks to prevent radicalisation and increase digital literacy amongst youth. This programme works both online (social media) and offline (theatrical performances and workshops). French Prime Minister Édouard Philippe convened the Committee in April 2019 following the Christchurch attacks to review the work done as part of the National Strategy Against Radicalization "Most initiatives are in the education sector and therefore managed by the regions and communities, according to the Belgium devolution of competences.

Examples implemented since the Christchurch call:
Organization of trainings to empower teachers confronted with fake news and conspiracy theories and on critical thinking for education and youth workers."

Belgium

and encourage further efforts. This work has been considerably re inforced following the October 2020 attacks in Conflans-Sainte-Honorine and Nice.

In addition, there were other approaches that do not fit easily into the above categories, reflecting the broad nature of this commitment. These include Iceland's development of legislation on equality, and clarifying the rules regarding "injunctions of expression". Similarly, Georgia has focused on equity of access to education, social support, and media for minority populations.

Given the wide range of approaches supporters noted, consistent reporting on monitoring and evaluation of different initiatives could be a useful future project.

This would enable the Call community to share what has been learnt about successful implementation of this commitment.

"The Government of Georgia has implemented several programs and projects to ensure ethnic and religious minorities' fully-fledged participation in all spheres of public life (including access to education, media and promoting equality). The respective initiatives are implemented by state agencies with the active engagement of international partners, civil society and human rights defenders."

Georgia (*)

Key question for the Christchurch Call community:

 Can best practices be shared across government to ensure that relevant media campaigns and educational initiatives effectively reach our population, including vulnerable communities?

¹⁴ https://www.hrc.co.nz/our-work/race-relations-and-diversity/give-nothing-racism/

¹⁵ https://www.agcom.it/

http://www.nohate.se/nohate.1295.html

https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper

¹⁸ https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html

¹⁹ https://www.cipdr.gouv.fr/

Second Question for Government Supporters: Legal Measures to Combat Terrorist and Violent Extremist Content

"Has your government taken action to ensure effective enforcement of applicable laws that prohibit the production or dissemination of TVEC, in a manner consistent with the rule of law and international human rights law, including freedom of expression?"

Relevant Commitment: 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.

A total of 17 out of 24 governments reported actions taken to meet this commitment.

Responses varied according to political systems. In the case of EU countries, responses varied according to the direction of EU-wide initiatives. Collectively, the responses show most governments are placing increased focus on ensuring the legislative measures implemented to address terrorism and violent extremism are fit for purpose in the online age.

Some countries rely on pre-existing or general legal frameworks. These include Japan, which criminalizes TVEC under an Act related to organized crime and control of the proceeds of crime, and Colombia, which utilizes laws from 2003 and 2006 that address the protection of data, and the prevention, detection, investigation, and punishment of financing of terrorism. The Colombian criminal code has also been utilized to prosecute offences relating to TVEC online. Malta uses existing laws to combat the promotion and dissemination of TVEC as well as the instigation of terrorist acts.

Another group, including countries directly affected by terrorism, has invested significantly in updating legislation that directly addresses terrorism and violent extremism. For example:

- Cyprus has updated counter terrorism legislation to include specific references to racism, hate, and extremism. This is made more effective when paired with specific legislation on using the internet to disseminate TVEC online or foster antipathy towards individuals or groups;
- Following a year-long review of Sweden's counter terrorism legislation, Swedish parliamentarians are now considering the inquiry's recommendations;

- New Zealand is working to address gaps in its legislative framework revealed by the Christchurch attacks, including provisions for the classification of "objectionable" material, which can include TVEC online. New provisions under the Terrorism Suppression Act (Control Orders) enables New Zealand authorities to place proportionate restrictions on persons convicted under the Act, which can include limiting access to electronic communications ²⁰;
- Germany is the only supporter that reported legislative approaches to a particular category of violent extremism, with the Act to Fight Right-Wing Extremism and Hate Crime. The Act contains a package of measures to provide a rapid and targeted approach to these issues. Germany also reported a range of multistakeholder initiatives to prevent the dissemination of hate speech via the internet, bringing together federal states, state media authorities, media outlets, and judicial authorities to improve consistency of prosecution of these offences; and
- EU member countries affirmed support for the current draft EU legislation on preventing the dissemination of terrorist content online 21, as well as the recommendations of Europol's Internet Referrals Unit (IRU).

"The European Commission proposed a new regulation to prevent the dissemination of terrorist content online in September 2018... The Regulation will enable EU member states to issue removal orders to hosting service providers (HSPs) and require HSPs to take proactive action to address the misuse of their platforms by terrorists"

European Commission

Italy has worked to increase protection for human rights through legislative means: An Italian Regulation (2019) on respect for human dignity and the principle of non-discrimination, and a further regulation (157/19/CONS) sets new rules for all media platforms – including online service providers – with regards to hate speech, violence, and discrimination.

Key question for the Christchurch Call community:

 While ensuring privacy and innovation, satisfying the requirements of all stakeholders, and remaining conscious of existing legal frameworks – what challenges and opportunities can be identified in the sharing of information and data related to the moderation of TVEC online?

Third and Fourth Questions for Government Supporters: Media Standards and Frameworks

"Has your government encouraged media outlets to apply ethical standards when depicting terrorist events online, to avoid amplifying TVEC?"

"Has your government supported frameworks, such as industry standards, to ensure that responsible reporting on terrorist attacks does not amplify TVEC?"

Relevant Commitment: 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 extremism.

After the Christchurch attacks, some media reporting of the incident included footage from the terrorist's livestream, increasing its reach for global audiences at the same time as technology companies were working to reduce harms by removing the content from their platforms. The intent of this commitment is to encourage governments to work with media to arrive at a shared understanding of the impacts of reporting on terrorist incidents with an online component, and effective approaches for reducing the risk of publishing TVEC.

A total of 12 out of 24 governments reported taking actions to meet these commitments.

- Portuguese officials have worked with media outlets to increase industry awareness of the risks of inadvertent amplification;
- The *UK Government* has has worked with mainstream media outlets to help them understand the unintended consequences of displaying graphic imagery or inadvertently republishing terrorist content;
- The *Government of Georgia* held a two day media seminar in November 2019, which included content on counter-narratives to terrorist propaganda, coordination between law enforcement and media during terrorist incidents and counter-terrorism operation, and sharing best practice and experience from the UK and EU countries;
- New Zealand government agencies have engaged with journalists to educate and encourage the application of ethical standards to future reporting on terrorist incidents; and

²¹ A political agreement has been found on this proposal since the completion of the consultation. The regulation is expected to be formally adopted by the Council and the European Parliament in February 2021:

https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2372

²⁰ The Royal Commission of Inquiry into the terrorist attack on Christchurch masjudain was publically released on 8 December 2020 (After the conclusion of the Community Consultation). The New Zealand Government has accepted all of the Royal Commission's findings, and has agreed in principle to all 44 of the Royal Commission's recommendations. For more information: https://christchurchattack.royalcommission.

• *Finland* regularly engages with journalists on issues and emerging trends related to countering violent extremism.

"The Ministry of the Interior organises regular gatherings with media representatives on topics related to P/CVE and terrorism. The latest discussion last March focused on the issue of violent right-wing extremism, including the symbols and narratives used in this context."

Finland

Several governments have invested in collaborating with likeminded partners on the sharing of best practice information for the responsible coverage of terrorist incidents.

- The *Canadian government* supports several non-governmental organisations that provide and/or highlight resources for media;
- The European Commission funds the European Strategic Communications Network²²
 through which EU member states share analysis, best practice, and ideas on the
 sustainable use of strategic communications in countering violent extremism. This
 network has engaged with media outlets on best practice when communicating
 terrorist events:
- In *France*, the Superior Council of Audiovisual's "code of conduct"²³ was born out of the 2015 and 2016 terrorist attacks, with parliamentary backing. The code of conduct was written after several meetings with representatives of the audiovisual media and journalists, as well as with experts, professional organizations, victims' representatives, and the Public Prosecutor of Paris. It takes into account reflections on progress and best practices in use within the editorial staff of audiovisual media services;

"After the 2015 and 2016 attacks in France, the French Media Regulatory Authority (CSA) encouraged media outlets to exercise caution, and was legally entrusted by Parliament to develop a 'code of conduct' relating to the broadcast coverage of terrorist events. The code was elaborated in concertation with the media industry, journalists and other stakeholders. It provides an overview of the issues raised by the coverage of terrorist events and proposes a set of precautions to address them."

France

- The UK government cites UNESCO quidance²⁴ when engaging with media outlets to make the case for removal of terrorist content, whilst reiterating its commitment to journalistic freedom; and
- The Government of Georgia maintains a website²⁵ providing credible counter-terrorism content to media as well as to wider society.

Some respondents cited regulatory requirements in response to this question:

- In Germany, media regulations state that providers must respect and protect human dignity and respect the moral and religious convictions of the population. News providers are also required to apply a sufficient duty of care with regards to verifying the sources of information; and
- Hungary reports that it has provisions under a 2020 amendment to the E-Commerce Act (2001) that requires the industry self-regulatory body to promulgate a professional code of conduct.

Reporting indicates that Call supporting Governments and (media) industry bodies have engaged with a common purpose to prevent the further dissemination of terrorist and violent extremist content, including through the development of various reporting guidelines and codes of conduct.

While a myriad of standards and guidelines now exist, it is not yet clear that these always filter down to frontline reporters, given that they may need to be applied in the fog of a terrorist attack, and taking into account the speed with which coverage is required of reporters. Furthermore, responses suggest there may be useful opportunities for enhanced reporter-level education opportunities and dialogue.

Examples provided by Finland and Georgia indicate welcome engagement at a domestic level. We see a clear gap in the education of reporters on international terrorism trends, TVEC online and the evolving threatscape, and in opportunities to consider these issues alongside peers from different cultures, social environments, reporting environments, and media models.

With the convening power of the Call and the global expertise it can call upon, the Call community might see scope for the development of more substantive programmes and dialogues to facilitate this.

²³ https://www.csa.fr/Reguler/Espace-juridique/Les-relations-du-CSA-avec-les-editeurs/Codes-debonne-conduite-et-textes-de-precautions-relatives-a-la-couverture-audiovisuelle/Precautions-relativesa-la-couverture-audiovisuelle-d-actes-terroristes ²⁴ https://unesdoc.unesco.org/ark:/48223/pf0000247074

Key question for the Christchurch Call community:

 What qualities of successful media standards and frameworks have been the most effective in managing instances of TVEC being amplified by the media?

Fifth Question for Government Supporters: Preventing Exploitation of Online Services from the Dissemination of TVEC

"Has your government taken action to prevent the use of online services to disseminate TVEC by developing regulatory and policy measures consistent with a free, open and secure internet and human rights?"

Relevant Commitment: 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; development of industry standards or voluntary frameworks; regulatory or policy measures consistent with a free, open and secure internet and international human rights law.

This particular question received a high ratio of responses returned, with 17 out of 24 country supporters confirming they had taken action to uphold this commitment. This is understandable considering every government supporter of the Call is inherently concerned by the dissemination of TVEC online, and seeks to mitigate the risk of TVEC impacting its population.

This particular commitment reflects the Call's understanding that action taken to eliminate TVEC online cannot be monolithic; it is subject to the domestic setting and context of individual supporters. The breadth of the question, and the nature of the relevant commitment, led to a wide range of answers with an array of multistakeholder initiatives, or legislation and cooperative efforts.

- Active negotiation of the <u>European Digital Services Act</u>²⁶ was referenced by *France* and *Belgium*. The Act is intended to tackle the moderation of illegal content more broadly and in accordance with a free, open, and secure internet;
- Malta referenced its Prevent Network, which brings together government entities with the aim of creating resilience and strengthening policy development on countering radicalization and violent extremism in all forms. The Prevent Network consists 16 government entities, all of which offer differing services in different areas;
- Australia has placed much of its efforts in multilateral and multistakeholder initiatives that compliment its domestic measures;

²⁶ https://ec.europa.eu/digital-single-market/en/digital-services-act-package

"Australia is advocating for an open, free and secure internet including the importance of protecting freedom of expression. For example, Australia supported the UN Human Rights Council (HRC) resolution on promotion, protection and enjoyment of human rights on the internet at the HRC in 2018. Australia is championing the Voluntary Transparency Reporting Protocol through the OECD that will create a common standard for digital platforms to report actions taken to remove violent extremist content."

Australia (*)

- New Zealand, France, Canada and the UK have also engaged in a number of multistakeholder forums, including the GIFCT Independent Advisory Committee ²⁷ the GIFCT multistakeholder forum and working groups within the organization; and
- Germany also mentioned having strengthened its commitments by requiring online service providers, especially social networks, to identify content automatically generated by a computer program (e.g. social bots).

This question had the effect of encouraging supporters to look at the "big picture" issue. Rather than referencing individual examples of actions taken, some supporting countries took this opportunity to showcase their government's general approach to TVEC issues and the values and principles that guide their day-to-day engagement.

"We support an effective cross-industry response, principally though the GIFCT's establishment as an independent NGO. In parallel, we're developing legislation to tackle online harms which will require companies to put in place appropriate systems to deal with harmful content on their services to keep users safe. Safeguards for freedom of expression have been built in throughout to ensure that internet users are protected whilst maintaining our commitment to freedom of expression and human rights."

United Kingdom (*)

Some recurring trends from the answers provided included:

- The development of multiple regulatory frameworks for social media platforms, including for the removal of illegal content, hate speech, and online harms; and
- The negotiation and development of the European Digital Services Act.

Key question for the Christchurch Call community:

 How can we best support the exchange of information on regulatory measures, industry standards and voluntary frameworks, and awareness-raising/capacitybuilding activities established within each supporting country?

Sixth Question for Government Supporters: Commitment Upheld Most Successfully

At the end of the section, governments were asked which commitment(s) they consider they have upheld most successfully, and why.

Many government respondents consider they have successfully taken appropriate actions to prevent the use of online services to disseminate TVEC. Relevant actions taken by governments include: supporting the reform of the GIFCT, developing online crisis response protocols, participating in the OECD negotiations on the voluntary transparency reporting of platforms, and increasing general collaboration with online service providers.

Some governments stated they have successfully strengthened – or are in the process of strengthening – their legal measures, by prohibiting the production or dissemination of TVEC via legislation. European respondents, for example, commonly cited the incoming EU regulation on terrorist content online.

Lastly, some governments indicate that they have successfully upheld the commitment on countering the drivers of terrorism and violent extremism by building more resilient societies. Malta has cited its Prevent Network, which aims to create resilience, and strengthen policy development to counter radicalization and violent extremism; Sweden has established the Swedish Center for Preventing Violent Extremism²⁸ to prevent ideologically-motivated criminality and terrorism.

Governments are also undertaking a range of activities domestically. The responses indicate there may be scope to build on the success of limited existing international exercises and collaborations. Governments may benefit from greater engagement with, or understanding of, the GIFCT and its practices.

Similarly, technical workshops and tabletop exercises, such as the international Crisis Response Workshop hosted by YouTube in New Zealand in 201929, provide further opportunities for stakeholders - including governments - to test the operation of their regulatory frameworks alongside international protocols, share operational expertise on crisis response, and strengthen networks of international responders.

Key question for the Christchurch Call community:

How can we ensure that momentum of the Christchurch Call continues in its third year?

2. ONLINE SERVICE PROVIDERS COMMITMENTS

All six company respondents outlined specific measures they have taken to prevent the upload, livestream, and dissemination of TVEC on their services. They all responded that they continue to increase transparency in their community standards or terms of services, enforce them in a manner consistent with human rights, and continue to review algorithmic operations that may amplify TVEC or drive users to such content.

The online service providers that support the Call³⁰ play a vital role in its delivery, being intrinsically involved in the problem we collectively seek to address. These companies are on the frontline of dealing with terrorism online. Our success depends in part on encouraging best practice from as wide a range of companies as possible.

Question One for Company Supporters: Prevention of TVEC Online

"Has your company taken transparent, specific measure to prevent the upload, livestream and dissemination of TVEC on social media and similar content-sharing services?"

²⁷ https://gifct.org/governance/ 28 https://www.cve.se/om-cve/in-english.html

²⁹ https://www.beehive.govt.nz/release/governments-and-tech-converge-strengthen-joint-responseonline-terror-events

³⁰ Amazon, Dailymotion, Facebook, Google, Microsoft, Qwant, Twitter, YouTube, LINE Corporation and Jeuxvideo.com

Relevant Commitment: 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.

All six company respondents said they have taken transparent, specific measures to prevent the upload, livestream and dissemination of TVEC on social media and similar content-sharing services. YouTube, Dailymotion, Facebook, Twitter and Microsoft focused on restrictions on their livestreaming services.

- YouTube updated its hate speech policies and placed restrictions on livestreaming. The company reviews the effectiveness of its policies and enforcement;
- Dailymotion restricted access to the livestreaming feature, limiting it to their most premium partners, who post content emanating from trusted sources;
- Facebook restricted Facebook Live from people who have broken certain rules on the platform, including as part of its <u>Dangerous Organisations and</u> Individuals policy³¹;
- Twitch recently updated its <u>community guidelines</u>³² to reinforce the company's zero tolerance policy on TVEC. It does not allow content that depicts, glorifies, encourages, or supports terrorism, or violent extremist actors or acts;
- Twitter automatised prioritisation of live video reports, and made improvements to their hash technology for uploaded images, videos, and GIFs. Twitter is also working to make increasingly better use of the hash database shared by industry partners, to improve content detection and policy enforcement efforts; and
- Microsoft, through the GIFCT, developed and managed a <u>Content Incident Protocol (CIP)</u>³³, enabling industry to act on livestreamed or broadcast content, resulting from a real-world terrorist or violent extremist event.

³¹ https://www.facebook.com/communitystandards/dangerous_individuals_organizations

³² https://www.twitch.tv/creatorcamp/en/learn-the-basics/community-guidelines/

³³ https://gifct.org/joint-tech-innovation/

"Twitter continues to invest in internal tools and technologies to detect and remove material promoting terrorism or violent extremism. We automated prioritisation of live video reports and made improvements to our hash technology for uploaded images, videos, GIFs and also better leverage hashes shared by industry partners to improve content detection and policy enforcement efforts. We also developed proprietary technology to proactively flag violent and gory content in media for human review and actioning, which guards against viral proliferation and copycat behaviour while ensuring we do not remove media that is documenting violence and potential human rights abuses."

Twitter

Since the launch of the Call the GIFCT's CIP has been activated on two occasions: the first on 9 October 2019 following video footage of a shooting in Halle, Germany, and the second on 20 May 2020 in response to video footage from a shooting in Glendale, Arizona.

In the Conflans attack, as the perpetrator did not livestream the attack and the content was deemed to be of relatively low-virality, the GIFCT companies did not initiate the CIP. The GIFCT has advised further work is underway on public communication in non-CIP scenarios and published a <u>statement</u>³⁴ on the organization's website regarding the response to the attack.

Key question for the Christchurch Call community:

 What can we learn from recent efforts of supporting companies to further develop transparent measures preventing the upload of TVEC, including its immediate and permanent removal, without prejudice to law enforcement and user appeals requirements? How can these efforts be supported by governments and civil society? Question Two and Three for Company Supporters: Transparency and Enforcement of Community Standards and Terms of Service

"Has your company provided greater transparency in the setting of community standards or terms of service?"

"Has your company enforced community standards/terms of service in a manner consistent with human rights and fundamental freedoms?"

Relevant Commitments: 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: prioritizing 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.

Call supporting companies described similar efforts to increase transparency in the setting of community standards/terms of service. Companies advised that this transparency is typically delivered via periodical self-evaluation reports. For example, YouTube publishes a quarterly Community Guidelines Enforcement Report. The report provides details about the flags the company receives and how they enforce company policies. YouTube has committed to make company policy easily accessible and expounded on conventional reporting by launching "How YouTube Works" in June 2020. This website provides YouTube's community with details about how the company seeks to act responsibly, including how it develops policies.

³⁴ https://gifct.org/2020/10/19/artificial-intelligence-and-countering-violent-extremism-a-primer/ 35 https://support.google.com/transparencyreport/answer/9209072?hl=en

"YouTube has clear policies in place and regularly evaluates their effectiveness. We remove content for violating the Community Guidelines. Channels or accounts may also be terminated. We make exceptions if a video is meant to be educational, documentary, scientific, or artistic (EDSA). The user is directly notified of a removal decision and is provided information about how to submit an appeal."

YouTube

Twitter referenced the expansion in 2020 of its terrorism and violent extremism policy to include violent organisations, or individuals who affiliate with and promote illicit activities. Twitter noted assessments under this policy are informed by national and international terrorism designations and by the company's violent extremist group and violent organisations criteria. The significant interface between national and international terrorism designations and company policy is evidence of the need for strong relationships and communication channels between stakeholder groups.

"In enforcing our policies Twitter seeks to strike the appropriate balance between public safety and free expression. To that end, our enforcement is guided by the necessity and proportionality principles embedded in human rights law."

Twitter

Separately, each of the company respondents advised that the manner in which they have enforced community standards/terms of service is consistent with human rights and fundamental freedoms. Some companies, such as Microsoft, have specifically established annual human rights reports, which include all the measures taken to respect and promote human rights, to ensure that technology plays a positive role worldwide. Others have recently updated the values that underpin their community standards to specifically reference human rights principles.

Some Call supporting companies have curated "Advisory Councils", and consult these human rights experts when developing new policies and products – or evaluating current ones – in an effort to better understand the impact of their platform.

From responses provided we noted that, in the establishment of community standards and community terms of service, one of the most important considerations is how these policies are presented. Consistently, company supporters acknowledged the importance of clear, simple communication of policies as key to ensuring positive engagement between company and consumer, consistent with human rights and fundamental freedoms. Additionally, company supporters make repeated reference to easily accessible ban appeal forms on each of their platforms. The ability to reconsider or reinstate accounts that have been removed in a clear way, is of vital importance to ensure that application of community standards and terms of service remains consistent with human rights and fundamental freedoms.

Key question for the Christchurch Call community:

 Are there opportunities for supporting companies to work more closely with civil society organizations, including the CCAN, in the development and implementation of community standards and terms of service, with particular regard to redress and complaints mechanisms?

Question Four for Company Supporters:

Reporting on Terrorist and Violent Extremist Content – Detection and Removal

"Has your company implemented regular and transparent public reporting, in a way that is measurable and supported by clear methodology, on the quantity and nature of TVEC being detected and removed?"

Relevant Commitments: 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.

All companies but one (five out of six) said they have implemented regular and transparent public reporting on the quantity and nature of TVEC being detected and removed.

- Facebook has updated the definition of terrorist or dangerous organisations, in consultation with counterterrorism, international humanitarian law, human rights, and law enforcement experts. According to the company, its new definition delineates and qualifies attempts at violence, particularly when directed toward civilians with the intent to coerce and intimidate. To inform the community about the quantity and nature of TVEC being detected and removed on Facebook, the company implemented regular transparent public reporting: the "Community Standards Enforcement Report³⁶". The latest report shows content actioned for terrorism increased from 6.3 million pieces of content in Q1 2020 to 8.7 million in Q2 2020 (driven by expanding proactive detection technology);
- Twitter has expanded its terrorism and violent extremism policy to include violent organisations or individuals who affiliate with and promote their illicit activities, in line with national and international terrorism designations and according to its criteria for violent extremist groups and violent organisations. Twitter has also implemented a way for people to report potential violations of this policy, whether they have a Twitter account or not. Twitter has established a comprehensive <u>Transparency Centre</u>³⁷, including updates to their tools and technologies to detect and remove terrorist and violent extremist content;
- Dailymotion has updated flagging mechanisms to facilitate the reporting process. It has implemented its Help Center³⁸ to protect users and provide guidance to report potential TVEC. It has also committed to implement transparent public reporting. For this purpose, Dailymotion has changed its internal mechanism to index TVEC reports and the decisions taken toward these reports;
- Microsoft publishes a bi-annual transparency report: the "Digital Safety Content 39 ", which includes information about how it works with international entities on these issues - for example within the GIFCT's Transparency Working Group or the OECD's "Voluntary Transparency Reporting Protocol". Microsoft encourages the reporting of content posted by - or in support of - a terrorist organisation and takes action on content (by suspending, if necessary, accounts associated with violations of their code of conduct). In addition, the company leverages a variety of tools, including hash-matching technology and other forms of proactive detection, to detect terrorist and violent extremist content; and

³⁶ https://about.fb.com/news/2020/11/community-standards-enforcement-report-nov-2020/

https://transparency.twitter.com/
 https://faq.dailymotion.com/hc/en-us

³⁹ https://www.microsoft.com/en-us/corporate-responsibility/digital-safety-content-report?activetab=piv ot 1%3aprimaryr3

 YouTube publishes a quarterly transparency report: the "Community Guidelines Enforcement Report", to provide details on content removals. It has also implemented a website to inform about their policies making process.

Individual transparency reports provided by companies provide an opportunity to share more information on the measures they take against TVEC, their appeal processes, and the results of these processes.

Some Call supporters consider that there would be benefit in a more consistent sector-wide approach to transparency reports and advised that they also contribute towards an OECD Experts' Group on Voluntary Transparency Reporting. This group aims at establishing a voluntary framework, specifying the type of data and information that companies could provide to improve transparency reporting on the actions they take against TVEC on their platforms.

Key question for the Christchurch Call community:

 How can supporting companies continue to improve on their commitments towards meaningful transparency in their reporting, and how can this be supported by governments and civil society?

Question Five for Company Supporters: Algorithmic Processes

"Has your company reviewed the operation of algorithms that may drive users towards and/or amplify TVEC in order to better understand possible intervention points and to implement changes where this occurs?"

Relevant Commitments: 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.

All companies said they had reviewed the operation of algorithms that may drive users towards and/or amplify TVEC, in order to better understand possible intervention points and to implement changes where this occurs. The approach to algorithmic processes differs from one company to another:

- Some, such as Facebook, report an increased focus on the restriction of hashtags, titles of pages or groups if they relate to dangerous organisations, militarised social movements, and violence-inducing conspiracy networks/ organisations; and
- Microsoft reports it has expanded the classifiers on the 'Bing' search that
 catch and block auto-complete suggestions for terrorist and other material.
 The company also expanded its list of terms related to TVEC online. This will
 inform counter-narrative contents when a user enters a query defined as a
 term related to terrorism and violent extremism:

"When Bing users enter a query from a defined list of more than 10,000 terms related to terrorism and violent extremism, they see video links to diverse counter-narrative content in the ads section at the top of the results page."

Microsoft (*)

- Others, such as *Dailymotion*, noted a focus on restricting and preventing the audience amplification of TVEC online by indexing and displaying only content uploaded by trusted partners;
- Twitter has worked to reduce the amplification of TVEC online by detecting and deamplifying toxic content with its machine learning model. This process involves sending the detected objectionable content to the content moderation team, which analyses the nature of the content and removes it if it violates Twitter's terms of service. If not, Twitter places an interstitial⁴⁰ over the content to warn users before viewing; and
- YouTube reports it has implemented a process to reduce recommendations
 of borderline content and continues to not allow terrorist or violent
 extremist content on its platform.

The "Content-Sharing Algorithms, Processes and Positive Interventions⁴¹" (CAPPI) Working Group of the GIFCT has established guiding principles for its work going forward and has developed a work plan and an agreed scope. Two subgroups have been set up to focus on the two issues the Working Group is tackling: Content-sharing algorithm processes, and positive interventions.

⁴⁰An interstitial is a web page displayed before (or after) an expected content page - in this context to confirm a user's age or comfort prior to showing age-restricted, objectionable, or potentially upsetting, material.

⁴¹ https://gifct.org/working-groups/

The CAPPI Working Group seeks to collaborate across industry, government, and civil society to map content-sharing algorithms and processes, to identify positive interventions and risk mitigation opportunities, while countering the consumption of specific content that could increase user interest in, or amplify terrorism or and violent extremism.

The CAPPI Working Group is co-chaired by Google/YouTube, New Zealand and the Brookings Institution. The CAPPI Working Group has been set up to be equipped to deliver substantially on Call commitments that address algorithmic outcomes. It will be up to every stakeholder invested in its success to ensure it does so.

Key question for the Christchurch Call community:

- How can supporting companies working with governments, academia, and civil society – provide more transparent insights into the function of recommendation algorithms, including where these may have unintended or harmful consequences?
- How can supporters work together on the development and delivery of "positive intervention" mechanisms to counter TVEC?

Question Six for Company Supporters: Commitment Upheld Most Successfully

At the end of the section, companies were asked which online service provider commitment(s) they believe they have upheld most successfully and why.

Company respondents referenced six different commitments that they believe were upheld most successfully, including:

- Transparency. Twitter believes that transparency is a key principle in its mission to protect the "Open Internet", and advancing the internet as a global force for good, which includes combatting TVEC on its service;
- Prevent the use of online services to upload and disseminate TVEC. Twitch
 has created mechanisms to ensure faster reaction, communication,
 and removal of TVEC, including: updating policies, adding clearer
 reporting mechanisms for TVEC, expanding the size and scale of
 moderation capabilities, and working closely with the GIFCT. These
 improvements were informed by an in-depth appraisal of what worked

and what improvements could be made after the Halle, Germany attack. Similarly, Dailymotion has put in place mechanisms to make its services less attractive for users of their platform who would upload TVEC, and have worked on "visibility and monetization" issues; and

Detection and removal of terrorist and violent extremist content. YouTube
explains that this commitment is having an impact. Between October and
December 2019, approximately 90% of the videos uploaded and removed
for violating their Violent Extremism policy were taken down before they
had 10 views.

In addition, supporters repeatedly referenced *the establishment of the GIFCT as* an independent organisation as an example of achievement. Four foundational goals guide the work of the newly independent GIFCT:

- To empower a broad range of technology companies, independently and collectively, with processes and tools to prevent and respond to abuse of their platforms by terrorists and violent extremists;
- 2. To enable multistakeholder engagement around terrorist and violent extremist misuse of the internet and encourage stakeholders to meet key commitments consistent with the GIFCT mission;
- 3. To promote civil dialogue online and empower efforts to direct positive alternatives to the messages of terrorists and violent extremists; and
- 4. To advance broad understanding of terrorist and violent extremist operations and their evolution, including the intersection of online and offline activities.

The successful restructure of the GIFCT to make it an independent organisation is consistent with the seventh voluntary commitment of the Call for companies to "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".

Key question for the Christchurch Call community:

 How can we best build a shared understanding among the multistakeholder community on the GIFCT's work, on how it can best deliver on its mission, and on how to enable the widest possible multistakeholder engagement in that work?

3. JOINT COMMITMENTS FOR COUNTRY AND COMPANY SUPPORTERS

Question One for Country and Company Supporters: Engagement with Civil Society

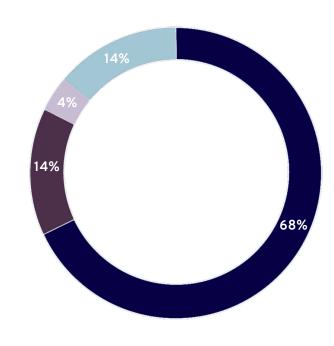
"Has your government/company worked with civil society promote community-led efforts to counter violent extremism in all its forms?"

Relevant Commitment: 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.

Company and country supporters were asked whether they had worked with civil society to promote community-led efforts to counter violent extremism in all its forms.

Respondents advised that supporters have developed of a wide range of initiatives to engage meaningfully with civil society. Respondents provided vastly different accounts of how they promoted community-led efforts to counter violent extremism. This section of the report offers an outline of approaches from country and company supporters, and points towards the need for further work in this area.

Has Your
Government
Worked with Civil
Society to Promote
Community-Led
Efforts to Counter
Violent Extremism
in All its Forms?



YES, ON A CONSISTENT BASIS

YES, PARTIALLY

NO INSUFFICIENTLY

NOT AT ALL

Figure 1. Responses from government supporters on work with civil society to promote community-led efforts to counter violent extremism, as percentages.

Recurring themes in the answers provided by governments included:

Counter-narratives and positive messaging
 In its response, Australia referenced a dedicated social media presence and consistent communication with civil society as beneficial to the building of trust between the government and population, while promoting an ethos of respectful online engagement through positive messaging.

In Portugal's response, a similar engagement model was described. The <u>PJ-UNCT</u>⁴² has actively participated in projects with non-governmental organisations, academics and law enforcement agencies, including those centered on the development and promotion of positive alternatives and counter-messaging.

• Sustained models of engagement

Other responses described a model of consistent engagement with civil society organizations. New Zealand and France meet monthly with representatives from the CCAN, a group of 44 civil society organizations from various backgrounds. These calls provide for ongoing, regular engagement between civil society and the governments on issues pertaining to TVEC online. It would be helpful to see this model of engagement extended to include a wider range of Call supporting governments and companies in the future.

Italy noted an established partnership between the Italian Ministry of Interior and religious communities to prevent radicalization through its "Pact for an Italian Islam⁴³". This National Pact has established a network for dialogue between the government and these communities, while also being described as a useful vehicle for the diffusion of positive alternative messages to TVEC online.

"Aside from building an important network for dialogue, it has created local roundtables that have allowed religious leaders to share information on how to identify those at risk for radicalization and to support and rehabilitate those individuals."

Italy

Financial support Canada and Sweden attributed financial support to relevant civil society organisations as an important method of ensuring meaningful development of community-led efforts.

Sweden also noted the funding of the "<u>Näthatsgranskaren</u>⁴⁴" (roughly translated as "Hate Speech Online Director"), who plays an active role in identifying hate speech online and reporting it to impacted companies.

The company supporters of the Call provided similar thematic answers to country supporters. This suggests that while the two stakeholder groups may have different motivators to their decision making, and inhabit vastly different working environments, the methods of engagement with civil society on issues related to TVEC do not differ drastically depending on whether you are from the private or public sector.

"The Canada Centre funds and supports civil society organizations that intervene with individuals at high-risk of radicalization to violence. This includes support for research, training, and best practices. Under the Community Resilience Fund and Digital Citizenship Initiative, the Government also supports civil society and community-led efforts to develop and promote alternative narratives. This includes support to communities impacted by online hate speech and violent extremism."

Canada

Has Your Company Worked with Civil Society to Promote Community-Led Efforts to Counter Violent Extremism in all its Forms?

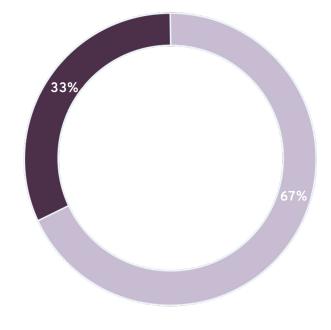


Figure 2. Responses provided by company supporters attributed to what scale they have worked with civil society to promote community-led efforts to counter violent extremism.

Recurring themes from company supporters' responses on how they have engaged with civil society included:

 Partnership with community and research groups for awareness raising/counternarrative purposes
 Companies have differed in their approaches, including targeted activities with individual groups and broader initiatives. Some appear directly related to the aftermath of the Christchurch attacks, while larger "umbrella" initiatives may take a more longterm approach to the issue.

"In New Zealand, we have engaged with community groups to support their advocacy and counter-speech work. In May 2020, we partnered with the Canterbury Muslim Community Trust to help their team spread awareness about Ramadan..."

Facebook (*)

Microsoft noted a three-year partnership with the Institute for Strategic Dialogue (ISD) on an intervention and education program for Bing users, with the intention of providing consumers with counter/alternative narrative content. Long term, collaborative partnerships like that between Microsoft and the ISD can provide a useful model for Call supporters who wish to initiate similar products.

Workshops and events
 YouTube and Facebook referenced the hosting of relevant workshops in their responses.

 Facebook has hosted multiple education sessions with community organisations in New Zealand, focusing on safety tools, counter-speech, and online community

engagement.

In December 2019, YouTube hosted an Incident Response Workshop in New Zealand. The purpose was to support an increased understanding and clarification of various protocols available to government, company, and civil society in crisis response, and to

⁴² https://www.policiajudiciaria.pt/unct/

⁴³https://www.interno.gov.it/sites/default/files/patto_nazionale_per_un_islam_italiano_en_1.2.2017.pdf

⁴⁴ https://näthatsgranskaren.se/

test these protocols in a controlled environment. An ancillary outcome from this event was the development of strong relationships between all stakeholders.

In-person events, including workshops and forums, provide important opportunities for face-to-face interactions between stakeholders. The current COVID-19 environment has limited the ability to meet outside of virtual environments. Despite this, a number of supporters have adapted to holding events virtually, including through the Aqaba Process and the inaugural Multistakeholder Forum of the GIFCT.

Key question for the Christchurch Call community:

 How can we improve engagement with civil society, and how can we encourage participation from organisations across a wide range of geographies?

Question Two for Country and Company Supporters: Information Sharing and Algorithmic Processes

"Has your government or company worked with other governments or companies to develop effective interventions, based on trusted information sharing, about the effects of algorithmic and other processes, to redirect users from TVEC?"

Relevant Commitment: 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.

The responses to this question from company and country supporters showed the initial impact that the restructured GIFCT has had on the shared understanding of algorithmic processes and development of effective positive interventions, and the potential for further, in-depth work.

- Membership, or observation of the CAPPI Working Group of the GIFCT was referenced numerous times by respondents, including Australia, France, Ireland, New Zealand, Twitter, Microsoft, and YouTube;
- Outlining its key role in the restructure of the GIFCT, Microsoft noted support for academic and practical research on counter-narratives, trends and patterns of online usage by terrorist and violent extremist networks, as well as the interplay between online and offline actions; and
- New Zealand highlighted the GIFCT's development of communication channels and information sharing among governments and companies into a structured multistakeholder model, referencing the CAPPI Working Group of the GIFCT.

Others supporters, including Germany, referenced new or refreshed legislation that sought to better understand the algorithms companies use, and promote constructive outcomes through positive messaging.

"The German federal states are in the process of implementing new legislation (Medienstaatsvertrag) which aims to improve the findability and accessibility of public value content. The criteria for making such content accessible will ... strictly adhere to the principles of independence/non-interference of the state regarding content-related issues of media outlets."

Germany (*)

Company responses typically depicted a greater diversification of owned (or supported) initiatives in this space, beyond the GIFCT. For example Twitter cited its membership of the "Online Hate Observatory", which is working on developing a better understanding of the mechanics behind online hate, in order to develop solutions in cooperation with non-governmental organisations, researchers, and relevant governments.

Facebook referenced a relevant body of work in this space, initiated in May 2019, when the company began connecting people who search for terms associated with white supremacy to resources focused on helping people leave hate groups. Originally this work, in partnership with the non-governmental organisation "Life after Hate", was limited to the United States. It has since expanded to more countries.

As outlined in the previous section, the CAPPI Working Group of the GIFCT was established in April 2020, in part to tackle issues pertaining to online algorithms as they relate to TVEC online, with the other topic of this Working Group being "Positive Interventions".

The objective of the multistakeholder CAPPI Working Group is to map content-sharing algorithms and processes to identify positive interventions and risk mitigation opportunities, while countering the consumption of specific content that could increase user interest in, or amplify, TVEC.

Key question for the Christchurch Call community:

- To what extent does countering the spread of TVEC online require modifications in the design of recommendation algorithms used by online platforms?
- How can we ensure the GIFCT's Content-Sharing Algorithms, Processes, and Positive Interventions (CAPPI) Working Group makes good progress based on trusted information sharing? How do we ensure the group's work is incorporated into the policy-making of companies?

Question Three for Country and Company Supporters: Technical Solutions

"Has your government taken action to research and develop technical solutions to prevent the upload of TVEC and to aid in its detection and immediate removal, drawing on expertise from academia, researchers, and civil society?"

"Has your company accelerated research into and development of technical solutions to prevent the upload of, and to detect and immediately remove TVEC online, and share these solutions through open channels, drawing on expertise from academia, researchers, and civil society?"

Relevant Commitment: 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.

In its submission, YouTube referenced the "first line of defense": the company's machine learning technology. This technology helps YouTube detect violent extremist content quickly and at scale. In the first quarter of 2017, 8% of videos removed for violating the violent extremism policy had fewer than 10 views at the time of removal, compared to approximately 90% in the fourth quarter of 2019.

Facebook invested USD 7.5 million in a university partnership to research new techniques to improve image and video analysis technology. Facebook noted a collaborative arrangement with government and law enforcement officials in both the United States and the United Kingdom to obtain camera footage from firearms training programs, to train Facebook's detection of real-world, first-person footage of violent events, and avoid incorrectly detecting other types of footage.

Government responses depicted a vast breadth of approaches, including the development of multistakeholder technical solutions. Canada is providing CAD 1.2 million to Tech against Terrorism (TAT) to develop the <u>Terrorist Content Analytics Platform (TCAP)</u>⁴⁵. The TCAP's purpose is to support smaller companies by providing a library of terrorist content, allowing them to better identify and remove content on their platforms. The TCAP is informed by academic research and TAT's advisory committee.

Responses indicate technical solutions are an important factor in the global effort to eliminate TVEC online and include a wide variety of tools and

processes, as indicated by the multiple different examples above. Responses received by governments and companies also reflect an important understanding that technical solutions are only one factor in the holistic approach required to address the problem of TVEC online.

Key question for the Christchurch Call community:

 How can Call supporters improve the research and development of technical solutions to prevent the upload of TVEC online, and enable its detection and immediate removal? How can that work best be shared through open channels to the wider community?

Question Four for Country and Company Supporters: Research

"Has your government or company supported research and academic efforts to better understand, prevent, and counter TVEC online, including both the offline and online impacts of this activity?"

Relevant Commitment: 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.

YouTube referenced the work undertaken by Jigsaw (a unit within Google), which conducts research with academics and builds technology to help identify and intervene in online recruiting by violent extremists. The "Redirect Method" – an open source program run by Google, Moonshot CVE, and others – uses targeted ads and curated YouTube videos uploaded by people all around the world to confront online radicalization. Twitter outlined the importance of collaboration between industry and academia.

We look forward to further joint efforts being explored between universities and the tech sector in the areas of terrorist/violent extremist content on their platforms.

"In a New Zealand first through our #DataforGood program, we entered into a partnership with the University of Otago's National Centre for Peace and Conflict Studies. Our shared goal is to use Twitter data to study the ways online conversations can be used to promote tolerance and inclusion instead of division and exclusion."

Twitter (*)

Microsoft referenced its support for the Academic and Practical Research Working Group of the GIFCT, as well as the academic research arm of the GIFCT: <u>The Global Network on Extremism and Technology (GNET)</u>. 46

"As a GIFCT member, Microsoft is supporting academic and practical research, including through the GIFCT Academic and Practical Research Working Group. The Global Network on Extremism and Technology (GNET) serves as the GIFCT's academic research arm, with the aim of better understanding the ways in which terrorists use technology. GNET's goal is to produce actionable outcomes, based on rigorous evidence-based research and robust academic methods."

Microsoft

Sweden pointed to research that the Center for Preventing Violent Extremism has conducted on symbols used by violent extremists online. This research has been utilized by those working to counter the actions of violent extremists, and has allowed for them to be better equipped in recognizing propaganda and the communications of violent extremists, both online and offline.

"Sweden's Center for Preventing Violent Extremism has compiled lists of symbols used in online and offline communication for practitioners to be better equipped to recognize violent extremist propaganda and messages online and offline. The Government has also tasked the Swedish Defence Research Agency to map and analyse violent extremist propaganda in digital environments. Both of these actions have increased the knowledge about the content of the propaganda and how it is used to recruit and radicalise individuals."

Sweden

Other governments have employed a range of techniques to develop research communities specialised in understanding, preventing, and countering TVEC.

- The *University of Malta* is part of the Prevent Network that aims at supporting TVEC policy development, thanks to its research and studies;
- *Italy* has chosen to sponsor research projects on online radicalisation and on international terrorism and extremism countering;
- Canada is involved among other initiatives in a multistakeholder project as a coleader of the GIFCT's Academic and Practical Research Working Group. ⁴⁷ Through this forum, Canada is working to improve researcher access to data and coordinate research activities: and
- Similarly, the *French Government* has worked with researchers to assess the radicalisation process and the utility of counter-narrative methodologies to face the issue.

"The Ministries of Interior and of Higher Education & Research have created the Scientific Committee on Preventing Radicalization (COSPRAD) in 2019 to facilitate interactions between gov authorities and researchers, to suggest priority research areas, and to translate academic findings into public policy. The database of radicalization reports was opened to accredited researchers. In parallel the CIPDR 48 asked a research team to carry out an evaluation of the cognitive impact of counter narratives."

France

These examples provided by supporters serve as evidence of the practical application that research into TVEC online can provide. They demonstrate positive efforts to better understand, prevent, and counter the offline and online impacts of this activity.

We look forward to further joint efforts being explored between universities and the tech sector in the areas of TVEC content on their platforms.

Key question for the Christchurch Call community:

How can governments and companies better facilitate research into technical solutions?
 How can they further their support of research and academic efforts to better understand, prevent, and counter TVEC online?

⁴⁵ https://www.terrorismanalytics.org/about

⁴⁶ https://gnet-research.org/

⁴⁷ https://gifct.org/working-groups/

Question Five for Government and Company Supporters: Cooperation with Law Enforcement Agencies

"Has your government or company cooperated with law enforcement agencies for the purposes of investigating and prosecuting illegal online activity in regard to detected and/or removed TVEC, in a manner consistent with rule of law and human rights protections?"

Relevant Commitment: Ensure appropriate cooperation with and among law enforcement agencies 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.

The majority of Call supporting companies have created guidelines, templates, or FAQs for law enforcement to use ⁴⁹, which serve as established systems of communication for the purposes of investigating and prosecuting illegal online activity in regard to detected and/or removed TVEC.

"We are ensuring a permanent cooperation with law enforcement agencies for the purposes of investigating and prosecuting illegal online activity in regard to detect and/or remove TVEC: We consider law enforcement agencies as 'trusted flaggers'. By this status, we give to their reports a high priority within our moderation process; if their report identifies, legally, content as TVEC, we systematically fingerprint this content to prevent any re-upload on our platform."

Dailymotion

While the question posed to company supporters was considered to be narrow in scope – relative to other commitments that allow for a certain degree of interpretation – the responses received on this question showed there are numerous ways tech companies work with law enforcement agencies. We can attribute the difference in approach from company to company to the well-established relationships already present between law enforcement and the tech sector, and how companies have each developed processes to be appropriate for the context of their business.

- Some companies, such as Facebook and Amazon, set Law Enforcement Guidelines to manage responses to law enforcement requests.;
- Twitter has an online tool the Legal Request Submission Site to streamline and expedite reviews;

- Besides its processes and procedures for responding to law enforcement requests, Google shares the number and types of requests it receives from governments in its Transparency Report ⁵⁰; and
- Microsoft has a legal department responsible for managing national agencies' requests.

"Microsoft has well-established process for engagement with law enforcement and national security agencies for the investigation and prevention of terrorist activities. Our Law Enforcement and National Security team is responsible for processing valid criminal and civil legal demand disclosures, in compliance with controlling laws and Microsoft policy. We disclose customer data only in response to a legally valid warrant, order or subpoena."

Microsoft

Government supporters provided similarly extensive responses to this question, indicating mature relationships between law enforcement and industry – consistent with best practice and the rule of law – to tackle TVEC online.

"Commonwealth, state and territory departments work closely with national regulatory and law enforcement agencies in addressing TVEC online under Australia's Criminal Code. The eSafety Commissioner works with law enforcement agencies nationally to facilitate the removal of TVEC and other illegal material hosted in Australia and overseas. The Attorney-General's consent is required before a prosecution can be commenced."

Australia

⁴⁸ Prévenir pour Protéger - Prévention Délinquance et Radicalisation (cipdr.gouv.fr)

50 Government requests to remove content - Google Transparency Report

⁴⁹ Facebook Law Enforcement Guidelines; Twitter Guidelines for Law Enforcement; Microsoft Law Enforcement Requests Report; Google Transparency Report Help Center (FAQs); Amazon Law Enforcement Information Requests

When objectionable content is hosted outside a government's jurisdiction, government supporters referenced well-established relationships with foreign counterparts to advise of objectionable content.

"Due to the global nature of terrorism, the significance of national and international cooperation has become more important than ever, in particular the real-time, efficient and proactive sharing of information between the affected countries. Therefore, TEK maintains continuous relations with the national and foreign partner services and cooperates with the involved organisations in the cases falling within its competence."

Hungary

Key question for the Christchurch Call community:

• In the event of an online crisis, how can government agencies better administer outreach to companies to ensure communication with the tech sector is consistent and clear, and that lawful requirements of law enforcement agencies are met?

Additional Question for Company Supporters Only: Support for Smaller Platforms

"Has your company supported smaller platforms to build capacity to remove TVEC?"

Relevant Commitment: 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.

In Twitter's response it referenced an ongoing partnership with "<u>Tech Against Terrorism</u>⁵¹", which – as part of the latter's commissioning from the <u>United Nations Counter-Terrorism Executive Directorate to tackle terrorist exploitation of technology</u>⁵² - works to support smaller tech companies with guidance on best practice in protecting their users.

"We support capacity building and information sharing with SMBs ⁵³ and startups working through the new GIFCT structure as an independent organisation led by an Executive Director and supported by dedicated technology, counterterrorism and operations teams. The GIFCT has conducted 11 separate workshops in partnership with United Nations Security Council Counter-Terrorism Committee (UNCTED) backed partner Tech Against Terrorism to facilitate outreach, knowledge sharing, and technology capacity build."

Twitter

The GIFCT's hash-sharing consortium is a database of "hashed" terrorist content. The GIFCT describes hashes as "unique digital fingerprints" of known violent terrorist imagery or terrorist recruitment video or imagery. Hashes appear as a numerical representation of the original content and can't be reverse engineered to create the image and/or video. Members can add hashes of content they have previously identified to be terrorist material on their platforms to the database, and can automatically detect terrorist material on their platforms and prevent its upload. Each consortium member decides how it uses the database (keeping in mind its own user terms of service, technical, and human capabilities). As YouTube notes in its response, the Consortium was set up by the four founding companies in 2016, and currently consists of 13 companies that have access⁵⁴ to the shared industry database.

"YouTube is a member of the GIFCT hash sharing consortium. The shared database currently contains more than 300,000 unique hashes, including videos and images. Since 2017, the number of companies benefiting from this database has grown from 4 to 13. Google is also a member of the GIFCT's Technical Approaches Working Group. The group brings together governments, industry and civil society to consider the technical requirements of smaller platforms and the availability of solutions."

YouTube

⁵¹https://www.techagainstterrorism.org/

 $^{^{52}\}underline{https://www.un.org/sc/ctc/wp-content/uploads/2015/09/CTED-press-kit-2016-ENGLISH.pdf}$

⁵³Small and midsize businesses

⁵⁴Microsoft, Facebook, Twitter, YouTube, Ask.fm, Cloudinary, Instagram, JustPaste.it, LinkedIn, Verizon Media, Reddit, Snap, and Yellow.

The GIFCT has published two <u>transparency reports</u> ⁵⁵ to date, providing insights on the hash-sharing database and the type of content added to it. In the 2020 report, the GIFCT said that the hash-sharing database contained content across the following categories:

- Imminent Credible Threat: 0.1%
- Graphic Violence Against Defenseless People: 16.9%
- Glorification of Terrorist Acts: 72%
- Radicalization, Recruitment, Instruction: 2.1%
- CIPs (Christchurch, 6.8%; Halle attack, 2%; Glendale attack, 0.1%)

The presence of a TVEC repository – created, contributed to, and curated by online service providers – serves as an important resource for smaller companies lacking the human or technical capacity to triage data uploaded onto their websites. It remains important that further development of the hash-sharing system continues to take into account human rights, including freedom of expression, and the important role of responsible reportage on terrorism and violent extremism. Enhanced transparency on how the hash-sharing process operates would assist in ensuring these principles are upheld.

Key question for the Christchurch Call community:

- How might smaller, Call supporting companies be better supported?
- What unique insights can smaller tech companies bring to Call supporting companies in the global effort to eliminate TVEC online?

Question Six for Government and Company Supporters: International Cooperation and Collaborative Actions Taken

"Has your government collaborated with partner countries, in the development and implementation of best practices to prevent the dissemination of TVEC online?"

"Has your company collaborated with partner countries and companies, in the development and implementation of best practices in the dissemination of TVEC online, in accordance with relevant data protection and privacy rules?"

Relevant Commitment: Collaborate, and support partner countries, in the development and implementation of best practice in 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.

Supporters referenced a large number of relevant initiatives that have seen companies and countries collaborate with others in the global effort to eliminate TVEC online. Specific examples referenced by company and government respondents included:

- The OECD's development of a <u>Voluntary Transparency Reporting Protocol</u> (<u>Framework</u>):56
- <u>The EU Internet Forum</u>⁵⁷, in collaboration with EUROPOL and the <u>EU Internet</u> Referral Unit;⁵⁸
- The <u>Agaba Process</u>;⁵⁹
- The UN Convention on Transnational Organised Crime⁶⁰; and
- Representation at the <u>Budapest Convention</u>⁶¹, the <u>Nordic Council</u>⁶² and the <u>Five Country Ministerial's "Digital Industry Engagement Senior Officials Group" ⁶³ (DIESOG).
 </u>

It was useful to see the scale of work adjacent to the Call and initiatives relevant to our collective work. The answers provided by respondents give a perspective on the breadth of work being developed concurrently in the global effort to eliminate TVEC online. It will be important for government and company supporters of the Call to avoid duplication of efforts as new initiatives are launched and existing measures are refined.

Key question for the Christchurch Call community:

- How can we ensure the Call's multistakeholder collaboration approach continues to develop in the long term? How can we ensure this approach secures support from a broader range of industry?
- What can be done to support partner countries, including those with limited capacity, in implementing the commitments of the Call?

⁵⁶https://www.oecd.org/sti/current-approaches-to-terrorist-and-violent-extremist-content-among-the-global-top-50-online-content-sharing-services-68058b95-en.htm

⁵⁷https://www.internetforum.eu/

⁵⁸https://www.europol.europa.eu/newsroom/news/europol-internet-referral-unit-one-year

⁵⁹https://www.un.org/sg/en/content/sg/statement/2020-09-02/secretary-generals-remarks-aqaba-process-virtual-meeting-covid-19-response-delivered

⁶⁰ https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

⁶¹https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/

⁶²https://www.norden.org/en

⁶³ https://www.thelawyersdaily.ca/articles/14325

Question Seven for Government and Company Supporters: Crisis Response

"Has your government or company taken action to develop processes allowing governments and online service providers to respond rapidly, effectively and in a coordinated manner to dissemination of TVEC following a terrorist event?"

Relevant Commitment: 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.

Three crisis response protocols are now operational that did not exist at the time of the Christchurch attacks. The Call's shared Crisis Response Protocol, the industry-led CIP, and the EU Crisis Protocol (EUCP). The development and continued refinement of these various protocols provides an interlinking network that enables governments, companies, and civil society to enact a rapid and coordinated response to online events. These protocols are complemented by domestic protocols developed by many countries.

- Canada is currently assessing the efforts of partner countries to develop crisis response protocols in order to inform the development of its own protocol;
- The Australian Government maintains that rule of law must apply online, and has worked closely with industry stakeholders to develop the Online Content Incident Arrangement (OCIA);
- The *United Kingdom* emphasised its work to improve the interface between protocols, as well as its domestic one; and
- To facilitate more seamless response, **Denmark** maintains a 24-hour point person to engage with the EUCP.

"Denmark is committed to the EU Crisis Protocol (EUCP), which is aimed at ensuring mechanisms to help coordinate cross-border response as well as cooperation with hosting providers in the event of a violent extremist or terror related incident, where TVEC related to the incident is being disseminated online. As part of this commitment Denmark has established a 24/7 point of contact responsible for securing a quick and efficient response if the EUCP is activated."

Denmark

The responses to this question from government supporters illustrated the strength and utility of considered, multistakeholder initiatives. This was consistently exemplified by EU member nations, who make up a significant portion of Call supporting countries (24 out of 48 – or 50% – of all country supporters). Respondents from these governments made repeated reference to their membership in, and utility of, the EU Internet Forum and the EUCP. The EU's Europol Internet Referral Unit (IRE) aims at anticipating and pre-empting terrorist abuse of online tools, and to play a pro-active advisory role vis-à-vis EU Member States and the private sector.

"We play an active role in the GIFCT's Crisis Response Working Group and supported the Christchurch Call Shared Protocol. Our priorities include: joining up current protocols, including by carrying out table-top exercises, to avoid duplication; and ensuring we learn lessons and evolve protocol accordingly following incidents. Beyond this, CTIRU (Counter-Terrorism Internet Referral Unit) has domestic protocols in place, including but not limited to a protocol to respond to a livestreamed attacks, which the Home Office is linked into."

United Kingdom

Call supporting companies have made concerted efforts to address and improve crisis response features and networks available to them since 2019. The CIP was created in April 2019 and announced in July 2019 in response to the Christchurch terrorist attacks.

"Microsoft spearheaded the development of the GIFCT's Content Incident Protocol (CIP). Through the CIP process, member companies can alert each other to, quickly assess, and act on potential content circulating online from a real-world event involving terrorism or violent extremism. Microsoft coleads the GIFCT Crisis Response Working Group, and we have engaged closely with governments on the development and testing of domestic and regional protocols."

Microsoft

As referenced in the responses from the United Kingdom and Microsoft, further collaborative work on crisis response is being carried out through the Crisis Response Working Group of the GIFCT. This Working Group has formed sub-working groups to ensure members' expertise and interests correlate to the relevant aspect of this multifaceted work.

Key question for the Christchurch Call community:

- How can the different crisis protocol frameworks be enhanced to ensure a holistic, well understood, and collaborative approach to online crisis management, which meets the needs of all stakeholders?
- Are there further creative opportunities for workshops focused on the operational multistakeholder response to a real life terrorist and violent extremist event with an online component?

Question Eight for Government and Company Supporters: Protection of, and Respect for Human Rights

"Has your government taken action to respect, and protect human rights in the context of work to prevent dissemination of TVEC online?"

"Has your company taken action to respect human rights?"

Relevant Commitment: 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.

Company supporters referenced the continued refinement of community standards and terms of service where reference is made to human rights principles.

- Guided by respect for universal rights, as laid out in the Universal Declaration of Human Rights, Google has integrated its commitments into its governance structure, risk management, and operational practices. Twitter also developed a governance structure

 a <u>Trust & Safety Council</u> 64 – that includes a dedicated Human & Digital Rights Advisory Group, to ensure the company respects human rights; and
- Microsoft and Facebook assess their human right commitments: <u>Microsoft's Annual Human Rights Report</u> 65, and the <u>Global Network Initiative's Biennial assessment</u> 66 of Facebook.

"In October 2019, we updated the values that underpin our Community Standards to specifically reference human rights principles. And earlier this year, the Global Network Initiative (GNI), of which we are a member, completed its biennial assessment of Facebook, which determined the company is making good-faith efforts to implement the GNI Principles with improvement over time. The assessor reported Facebook had "strengthened its systematic review of both privacy and freedom of expression."

Facebook

This question also prompted company supporters to provide further examples of collaborative engagement – including with advisory groups they work with to develop policies – to ensure they understand and address the potentially devastating harm online services can inflict on enjoyment of a wide range of human rights.

"Twitter is used by human rights activists and social movements worldwide, and elevating such voices is core to our mission. Our Trust & Security Council includes a dedicated Human & Digital Rights Advisory Group. We regularly consult with human rights experts when developing new policies and products, and to better understand the impact of our platform and the kinds of content that could increase risk of harm to a range of human rights."

Twitter

Government respondents typically focused on the development of new domestic policies and online governance that make specific reference to the protection of human rights in cyberspace.

 Canada reported the design and launch of a Digital Charter to enumerate the guiding principles of the country's digital policy.

⁶⁴https://about.twitter.com/en/our-priorities/healthy-conversations/trust-and-safety-council

⁶⁵https://www.microsoft.com/en-us/corporate-responsibility/human-rights

⁶⁶https://globalnetworkinitiative.org/tech-and-telecom-companies-make-progress-implementing-the-global-network-initiatives-principles-on-freedom-of-expression-and-privacy/

"Canada has launched its Digital Charter, the foundation for a Canadian approach that guides policy development and implementation. The Charter's 10 principles lay out the framework for online governance inclusive of protections for human rights. Canada is also creating a policy on digital inclusion, which will help guide Canada's digital foreign policy. Canada is also a founding member and contributor to the Freedom Online Coalition, which is committed to supporting internet freedom."

Canada

Other supporters took this opportunity to reaffirm a strong commitment to upholding international human rights law, and reflecting this sentiment through recently developed domestic legislation.

- Recognising the importance of a free, open, and safe internet in ensuring human rights, France initiated the <u>Charter for a Free, Open and Secure Digital Transformation</u>⁶⁸ during its G7 presidency in August 2019. France is careful to ensure these principles are taken into account in current and future regulations; and
- Ireland showed support for upholding the United Nations' Guiding Principles on Business and Human Rights as a foundational benchmark for the protection of human rights in its response.

"More generally Ireland's support for the three pillars of the United Nations Guiding Principles on Business and Human Rights of the States' duty to protect, corporate responsibility, and access remedy is reflected in Ireland's first National Plan on Business and Human Rights (2017-2020). More specific to TVEC is the inclusion of duty of care and right to redress provisions in the proposed EU Regulation to prevent the dissemination of terrorist content online."

Ireland

Key question for the Christchurch Call community:

 How can Call supporters assist each other in ensuring implementation is consistent with respect for international human rights law, fundamental freedoms, and a free, open and secure internet? How might we be more active in this?

Question Nine for Government and Company Supporters: Joint Commitment Upheld Most Successfully

Call supporting countries and companies were asked which joint commitment they believe they had upheld most successfully and why.

One of the recurring themes from the answers provided by both government and company supporters of the Call was a recognition of their organisation's concerted effort to deliver the Call approach of collaborative, multistakeholder action to eliminate TVEC online.

"We are proud of our efforts to champion a collaborative, multi-stakeholder approach to tackling TVEC whilst maintaining FoE. We supported the GIFCT as it transformed into an independent NGO and championed the involvement of a diverse range of countries, companies and CSOs. We play a leading role on the IAC, co-chairing the Tech Approaches WG, and as part of the Crisis Response WG. Beyond the GIFCT, we have worked closely with Five Country partners to increase the effectiveness of the DIESOG⁶⁸."

United Kingdom

Similarly, some supporters referenced how the work of the Call relates to the context of their own domestic setting, and how increased cooperation with other governments and companies had been seen as a key outcome.

"International cooperation. Historically in Latvia there has been limited number of cases where terrorist or violent extremist content has been disseminated on servers based in Latvia. Therefore most significant activities in this area are related to international cooperation. In particular regarding initiatives of EU."

Latvia

Understandably, several company supporters made reference to their key role in the reform of the GIFCT and the development of GIFCT associated products, including the CIP.

"We have been most successful in developing and implementing processes that allow companies and governments to respond quickly to situations in which online services are being used to disseminate TVEC. The GIFCT Content Incident Protocol requires stakeholders to work together to solve the difficult problems involved in communicating in a crisis, including: agreement on communication channels, sharing technology, and building trust among the companies involved."

Amazon

Some supporters went as far as acknowledging that there is not likely to be a definitive end to the work in this space, as terrorism and violent extremism and its manifestations online change and present new challenges for the Call community to address.

"We know that our work in this area will never be done, but we have undertaken continuous efforts to respond to the evolving TVEC environment and worked to produce solutions appropriate to our business. We have been most successful in effectively working with industry through coalitions, such as the GIFCT, to share this knowledge and leverage our learnings across companies. We continue to explore additional avenues to harness innovation for greater good across shared problem sets."

Twitter (*)

V. Progress and next steps

1. ACHIEVEMENTS OF THE CHRISTCHURCH CALL

What have been the main achievements of the Christchurch Call since 15 May 2019?

Significant work has been accomplished since the launch of the Call by French President Emmanuel Macron and New Zealand Prime Minister Jacinda Ardern. Respondents identified four main achievements of the Call:

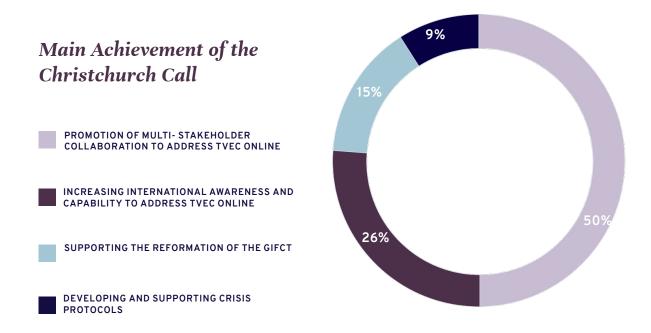


Figure 3. Responses provided by supporters and the CCAN on what they believe the greatest achievement of the Call has been to date.

A. Promoting a unique, multistakeholder approach to preventing the abuse of the internet by terrorists and violent extremists. 50% of responses referenced, in some capacity, the unique multistakeholder approach embraced in the development and implementation of the Call. For the first time, governments, major tech companies, and civil society representatives have created an innovative, flexible coalition, working cooperatively to stop and prevent attacks like Christchurch being broadcast and spread online.

The Call community has recognised the need to harness tech companies' creativity and technical know-how to co-design smart solutions, while ensuring internet freedoms are maintained, and that the internet is protected as a force for good.

Government and company supporters referenced the Call's promotion of meaningful engagement with civil society and non-governmental organisations. By supporting the Call, supporters have committed to upholding a free, open, and secure internet as a fundamental global good, and to the protection of human rights and fundamental freedoms, including freedom of expression. Civil society voices have been recognized by supporters and members of the CCAN as key to maintaining accountability for these outcomes, and to engaging the perspectives and expertise of civil society in implementation.

B. Raising awareness of the need to tackle TVEC online. 26% of respondents referenced, in some capacity, the ability of the Call to raise global awareness of the need to protect the internet from exploitation by terrorists and violent extremists, and from the dissemination of TVEC online. The Call is now supported by 48 countries, the European Commission, two international organisations, and ten technology companies. The 44 members of the CCAN – many of whom have been engaged on the Call since its launch – provide ongoing advice on the implementation of Call commitments and contribute strongly to the growth in awareness of the issues posed by TVEC online.

Specific examples provided by the Call community of awareness-raising include references to the promotion of multistakeholder workshops (e.g. the December 2019 Incident Response Workshop held in Wellington, which brought government, industry, civil society, and academia together to brainstorm potential solutions over the course of two days).

The Call community was separately asked what level of understanding they possessed on work currently underway under the Call. 69% of supporters reported their understanding at above average. It will be important for New Zealand and France, as co-founders, to continue efforts to engage the wider the Call community in its work, in particular with those stakeholders who reported an "average" understanding of Call.

C. Supporting the restructure of the Global Internet Forum to Counter Terrorism as an independent, multistakeholder organisation. 15% of respondents referenced, in some capacity, the role the Call played in the restructure of the GIFCT, and the role it continues to play in supporting the GIFCT's three strategic pillars⁶⁹.

The Call has been recognised by respondents as a catalyst in the reform of the GIFCT, an initiative originally set up in 2017 by Facebook, YouTube, Microsoft, and Twitter to help address terrorist content on their platforms.

In a meeting at UNGA 74, September 2019, industry leaders and Call supporting governments announced⁷⁰ the plan to reform the GIFCT into an

⁶⁹ https://gifct.org/

⁷⁰https://www.beehive.govt.nz/speech/remarks-christchurch-call-leaders%E2%80%99-dialogue

independent organisation, which was acknowledged by Prime Minister Ardern as a substantial, meaningful commitment by industry.

The reformed GIFCT is now an independent organisation with its own executive director, a 24/7 crisis management function, a set of working groups⁷¹ covering a wide range of topics, and a programme of multistakeholder engagement. An Independent Advisory Committee⁷² – including membership from civil society, government, and intergovernmental organisations – provides advice to the GIFCT on its strategic direction and work programmes.

D. Developing and implementing crisis response protocols to prevent the dissemination of TVEC online in the aftermath of a terrorist attack. Nine percent of the Call community acknowledged that the development of protocols and enhanced communication processes established between companies, law enforcement, and relevant government agencies has made a positive impact on the ability to limit the dissemination and virality of TVEC following an attack. Areas for improvement and ongoing development remain.

The Call community noted the continued refinement of the Call's shared Crisis Response Protocol⁷³ as a key achievement of the Call. The Crisis Response Protocol is a living document, with the purpose of ensuring coordinated and rapid action by online platforms and endorsing governments to counteract the spread of TVEC online in the event of a terrorist attack with an online component. The protocol, developed in consultation with a multistakeholder group, establishes common thresholds that respect free speech and human rights, and incorporates provisions for transparency and redress.

Members of the Call community referenced the GIFCT's CIP in their responses. The CIP serves as a standalone industry process, designed to be easily integrated into external crisis response procedures. By declaring a CIP, all hashes⁷⁴ of an attacker's video and other related content is shared in the GIFCT hash database with other GIFCT member platforms. Furthermore, a continuous stream of communication is established among all GIFCT founding members to identify and address risks and needs during an active CIP.

The EUCP⁷⁵ was referenced by the Call community as another example of the development of crisis protocols since the Christchurch attacks. The EU Crisis Protocol is a voluntary mechanism to help coordinate a rapid, collective, and cross-border response to the viral spread of TVEC online. Participants of the EU Crisis Protocol include EUROPOL and EU member nations.

2. HOW EFFECTIVE HAS THE CHRISTCHURCH CALL BEEN SO FAR

The Call community was asked how effective it believed the Call has been in addressing the dissemination of TVEC online since its inception in May 2019. Of the 34 respondents who answered this question, the majority (59%) consider its effectiveness to date as either "good" (38%) or "very good" (21%). The remainder noted in their responses that the Call requires additional commitment and action from its supporters. More than half of the respondents from the CCAN consider further commitment and concrete action is required before they are able to rate the Call's efficacy higher than "average".

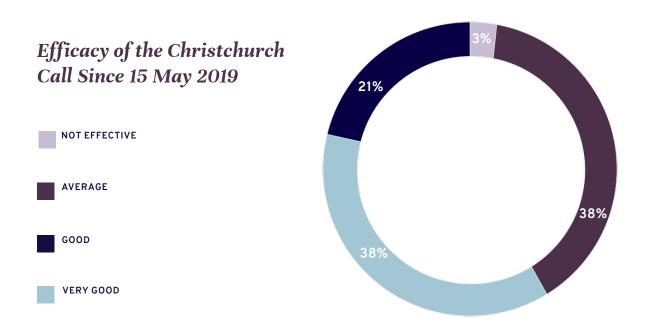


Figure 4. Responses provided by supporters and the CCAN on how effective they believe the Call has been to date.

While a slight majority of all respondents rated the Call's effectiveness as at least "above average", it will be important for New Zealand and France, as co-founders of the Call, to respond to the views of the 42% who believe further action is required, in order to ensure the initiative continues building on the early achievements recognised by the Call community in Figure 3. This will require a doubling-down on the work of the Call, taking into account suggestions for the Call's future raised by supporters and the CCAN. This will include how best to engage civil society and the wider Call community in ongoing work under the auspices of the Call. The release of the final report on this inaugural Christchurch Call Community Consultation is one step to assist in addressing this, providing a valuable baseline for future work.

3. NEXT STEPS FOR THE CHRISTCHURCH CALL

Respondents were asked to provide their perspective on the main areas of focus for the Call's ongoing work. The following graph sets out the Call community's responses:

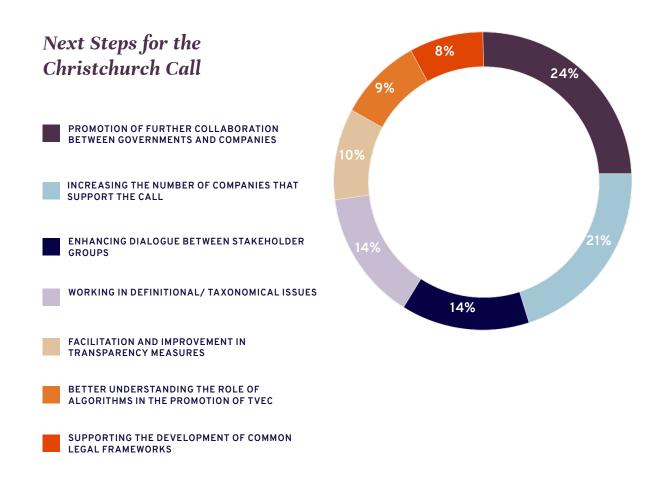


Figure 5. Supporters and members of the CCAN responses on what the next steps for the Call should be going forward.

⁷¹https://qifct.org/working-groups/

⁷²https://gifct.org/governance/

⁷³New Zealand and French officials are currently addressing and implementing the third round of multistakeholder feedback on the shared Crisis Response Protocol.

⁷⁴A hash in this context is the 'digital fingerprint' of content. The process of hashing involves converting a given key into another value, according to a mathematical algorithm, which in the case of the GIFCT's hash sharing consortium, can then not be converted back to its original key.

⁷⁵ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf_

A. Promoting further collaboration between governments and companies: 24% of respondents advised in responses to this question that the recognised greatest achievement of the Call (Figure 3. the promotion of a unique multistakeholder approach) should remain an ongoing focus for Call work.

Opportunities for collaboration between governments, companies, and civil society under the Call, include for example, table-top exercises or workshops focusing on crisis response, similar to the Incident Response Workshop hosted by YouTube in Wellington, December 2019.

B. Increasing the number of companies that support the Call:

21% of respondents indicated an understanding that platforms owned by technology companies are susceptible to exploitation by TVEC, and as such are uniquely placed to prevent and respond to its dissemination. Increasing company support for the Call will serve to improve the efficacy of the Call, as commitments are adopted and actioned by a larger portion of the technology industry, including small and medium sized companies.

The addition of LINE and jeuxvideo.com to the growing list of Call supporting companies in 2020 was a welcome step in expanding company support since the Call's announcement. New Zealand and France will continue working in 2021 to ensure the Call community seeks support from a broader range of online service providers interested in the global effort to eliminate TVEC online.

C. Enhancing the dialogue between stakeholder groups:

14% of respondents referenced the need to enhance the quantity and quality of dialogue between the different stakeholder groups that make up the Call community. In particular, respondents noted the need to ensure civil society is well engaged on how Call supporters are delivering on their commitments and that ample opportunity is provided to allow for expert advice and support by the CCAN.

Similarly, respondents proposed that New Zealand and France, as co-founders, should work to reinforce trusted relationships with members of the CCAN, to support the CCAN in providing meaningful guidance and impactful work.

D. Working on definitional/taxonomical issues:

14% of respondents noted a desire to see the Call community work on developing a common and precise definition of TVEC.

Respondents acknowledged the work to address these issues currently underway within the Legal Frameworks Working Group of the GIFCT.

E. Facilitating an improvement in transparency measures:

10% of respondents indicated that an increase in transparency on all fronts was required. Examples provided included greater transparency on behalf of governments in their interactions with the CCAN, greater transparency on behalf of online service providers reporting on the impact of TVEC on their platforms, and greater transparency in the setting and implementation of Call supporting companies' terms of service and community standards.

F. Better understanding the role of algorithms in the promotion of TVEC online:

9% of the respondents want to see a renewed focus on the role of platform design, systems, and technical architecture in the dissemination of TVEC online.

Specific examples were provided on the role of recommendation algorithms in connecting disparate far-right groups online, and engaging users in harmful content.

G. Supporting the development of common legal frameworks:

8% of the respondents advised that differences in the legal frameworks of the various countries, including on data protection and protection of rights such as freedom of expression, posed one of the greater challenges in sharing data and working on solutions.

Supporters noted that the country in which the online service provider is established can be particularly influential in this regard.

VI. Conclusion

New Zealand and France reaffirm our shared commitment to the Christchurch Call, and commend the work of supporters to date. As co-founders we look forward to building on work outlined in submissions provided by the Call community to eliminate TVEC online.

Consistent with the principles of the Call, the 2020 Community Consultation was a multistakeholder effort to provide an overview on how supporters are implementing the voluntary commitments agreed to in Paris and New York. Participants agreed to open-source their answers, in accordance with the joint commitment to collaborate in the development and implementation of best practice in preventing the dissemination of TVEC online. The answers provided by the Call community are available, in full, on the Call's website.

The responses to this exercise highlighted the positive impact of work undertaken by Call supporters to tackle TVEC online. In less than two years, the Call has enabled essential developments consistent with its commitments, such as the reform of the GIFCT, and the implementation of various crisis protocols. The Call, through its multistakeholder format, has enhanced dialogue between supporting governments, technology companies, and civil society. It has made a significant contribution to how the multistakeholder approach is addressing this global problem in a way that is transparent and consistent with international human rights law and fundamental freedoms, including freedom of expression.

This report has highlighted a number of areas for ongoing work – for doubling-down on our efforts as a community. There is much in the existing work that can be further progressed, and recent developments in terrorist and violent extremist exploitation of the online environment indicate the importance of evolving and adapting our shared work under the Call's commitments. As the Call heads into its third year, New Zealand and France will engage with the wider Call community to consider these areas of focus and enhance the ongoing work of the Call.

While much progress has been achieved by the Call community in the 20 months since its launch, it is clear that much more remains to be done. Recent terrorist attacks with online components in France, Austria, and elsewhere have underlined once again that malicious actors continue to search for new

ways to promote terrorism and violent extremism online. This has real world consequences. The murder of a school teacher last October in Conflans-Sainte-Honorine, followed online incitement to violence, and was amplified by the perpetrator's abuse of the internet, seeking to glorify their actions before a global audience.

As this report indicates, the multistakeholder, comprehensive approach in the Christchurch Call is an important element in addressing the ongoing challenges posed by terrorist and violent extremist content, including content distributed after an attack, glorifying terrorist and violent extremist acts or inciting such violence.

For as long as these malicious actors continue to look for new ways to exploit the internet, the Call community will be working to counter them – together.

The Call is an opportunity born of tragedy; it supports the idea that constructive, multistakeholder partnerships can deliver positive solutions.

It is a shared responsibility to do the right thing by the victims of the Christchurch terrorist attack and others like it, through preventing further harm resulting from all forms of TVEC distributed online.