Voices For Action Note

On Tuesday 14 May New Zealand hosted civil society representatives (see attendee list below) at the OECD in Paris to discuss the Christchurch Call. The first session (of approx. two hours) featured a briefing by MFAT and DPMC officials and individual table-based discussions on the key themes of the Call.

The Prime Minister joined the group during these discussions, and participated in conversations at some of the table. Following this, the PM took questions from the floor for around an hour, before the event concluded with a reception.

Some of the key themes to emerge from the discussion included:

Process, Freedoms and Human Rights

A number of speakers criticised the process for engaging civil society to date. They expressed concern that the text had not been consulted more broadly with civil society representatives. Going forward, there should be a policy of "nothing about us without us"

Several speakers commended the inclusion of human rights in the text, but noted that there would always be a tension between rights and freedoms and this issue. (Comment: though few had solutions to this problem).

Definitions

One of the key issues that stifled international – and even domestic – progress on this problem was that of definitions of terrorist content. Was there a way to do this that was not about wordsmithing, but that somehow harnessed technology to create an adaptive, normative approach to what is and isn't acceptable content?

Even if agreeing internationally on definitions would be difficult, there was merit in agreeing definitions across platforms. Platforms could also agree to share community standards, to improve interoperability and clarity for users.

Other country partners

Several speakers raised concerns about the Call being used by countries looking to justify repressive acts. s6(a)

The PM noted that all countries would need to meet the commitments outlined in the Call, including with respect to freedom online.

One speaker s9(2)(ba)(i) wondered whether one way to manage this risk would be by engaging civil society groups from "riskier" countries in dialogue about the Call, and involving them in civil society processes going forward. This may mean that those governments are less likely to engage in a process endorsed by such groups.

We were encouraged to "reach out to Africa" as we broadened the Call.

Working with Tech companies

The s9(2)(ba)(i) commented that, from its experience, a collaborative approach with the tech companies was the right one to take. A legislative/regulatory approach did not deliver the right outcomes.

s9(2)(ba)(i) made a pitch for working to build the capacity of smaller platforms who were unable to deal with a lot of this content themselves. s9(2)(ba)(i) said that we (NZ) needed to make sure we were working with those in the companies that knew what was possible from a technical and business standpoint – not just policy representatives.

The Business Model

It would be difficult to address the issue of terrorist and violent extremist content online without addressing the business model of the companies concerned. This was at the heart of the promotion and amplification of the kinds of messages that led to radicalisation and sharing of violent extremist content. Countries needed to ask whether they were doing enough to ensure that the business model was responsible. For example, should algorithmic manipulation services be legal? And what pressures were being brought to bear on those countries that hosted users/services (e.g. sock puppets; bots) that amplified these effects?

s9(2)(g)(i)

Algorithms

It would be important to be clear with tech companies that "we don't want to see the recipe… we just want to know what's on the label" with regard to algorithms. This should be possible. s9(2)(ba)(i)

The companies themselves should be encouraged to do forensics on this issue – too many had no capacity to do so.

It would be important to look at how algorithms could be/had been exploited, as well as how they amplify/promote content.

Not all about the take-down

We were encouraged to think of innovative responses to the issue – not just about removal and prevention.

The broader issue

It was difficult at times to focus the conversation on the specific issue of terrorist and violent extremist content online – many participants wanted to talk about the broader issues of radicalisation and root causes of terrorism.

Key Practical Takeaways:

- Cooperation across tech companies, countries and civil society is currently poor, and there is no obvious forum in which to try to improve it. **New Zealand could consider acting as a broker to bring these groups together**. This should be at the working level, to drive constructive, solutions-focused change.

- There was scope for a **central body to better coordinate responses to this issue**, and to work with trusted researchers to better understand the problem. This would involve sharing data – but this could be managed through developing trust, and clearly articulating our ask/purpose. The GIFCT was perhaps where this could start, but it needed to be far more transparent and with structure put around it. It also needed to have measures for success. The convening structures that had been created for online child sexual abuse were good models to consider emulating (e.g. National Centre for Missing and Exploited Children) – they collected data and shared this to develop response mechanisms, including with researchers. Trust would be critical to this for the companies – something that New Zealand seemed to be developing.

- In order to actually address this problem, you need to know which bits of it to tackle, and in what order. We need to "**map the hydra**" before we start lopping off heads. Approaches should be evidence-based.

- Terrorist use of the internet and the changing face of terrorism (e.g. increase of white nationalism) is a rapidly evolving issue. There is expertise in civil society, but not resource. Consider working with tech companies to establish **third party funding mechanism for research.**

From: DS MLG
Sent: Friday, 19 July 2019 5:35 PM
To: ALL POSTS (FM)
Cc: FM.P/S MFA (Seemail); FM.DPMC (FPA) (Seemail); FM.DPMC (NCPO) (Seemail); FM.P/S Communication & Digital Media (Seemail); FM.P/S NZSIS/GCSB (Seemail); FM.MBIE Formal Messages (Seemail); FM.NAB (Seemail); FM.Internal Affairs (Seemail); FM.Police (Seemail); FM.Justice Ministry (Seemail); DS AAG; DS EMA; DS TEG; DCE; CEO; ALL POSTS (FM); MEA; EUR; AUS; ECO; TND; NAD; SEA; ARD; ISED; LGL; UNHC; CMD; AMER; ECO
Subject: FORMAL MESSAGE: CHRISTCHURCH CALL: BAY AREA ENGAGEMENT 10-12 JULY AND CRISIS PROTOCOL WORKSHOP IN PARIS 9 JULY
Attachments: FILE NOTE - Detailed discussions on Christchurch Call 10-11 July.docx

Security Classification:

Not for cable exchange.

Summary

Two months have passed since the Christchurch Call to Action to eliminate terrorist and extremist content online – a series of follow-up meetings with the key tech company supporters in San Francisco, 10-11 July, provided an opportunity to reinforce our expectations on delivering progress against the Christchurch Call before Leaders' Week.

s9(2)(ba)(i)

s9(2)(ba)(i)

In addition to this engagement, we also convened a workshop in Paris to further develop thinking on a crisis response protocol; and hosted an open discussion with civil society on next steps for the Call.

Our next key milestone will be the GIFCT Conference on 24 July in Silicon Valley, where we will be looking to substantively progress discussions on GIFCT reform and on crisis response.

Action

For information.

Report

As agreed in the margins of the recent Aqaba Process technical meeting in Amman (DS MLG's FM of 28 June refers), Victoria Hallum, Paul Ash (DPMC) and Liz Thomas had a series of discussions in San Francisco, 10-11 July, focused on next steps in implementing the Christchurch Call. This included a roundtable discussion with the key tech industry Call supporters; met individually with Facebook, Twitter, Google and Microsoft; and hosted a workshop with civil society. Murray Bruges (LOS) also attended the meetings.

2 These discussions with the tech companies were critical in testing companies' ability and determination to deliver substantively on Christchurch Call commitments – and to show meaningful progress by United Nations General Assembly (UNGA) Leaders' Week in late September. Our objectives for these meetings included: registering our expectation that the 24 July Global Internet Forum to Counter Terrorism (GIFCT) conference would be a key milestone; having a substantive and concrete discussion about next

steps on delivering the Prime Minister's priorities (especially on structural options to take forward the Call, whether through the GIFCT or a new construct); and to ensure the companies understood our intentions for joint announcements on meaningful progress during UNGA Leaders' Week in late September.

3 Our programme included standalone meetings with Facebook, Twitter, Microsoft and Google, plus a larger roundtable with the four key tech companies, hosted by Facebook and including French and UK officials. s9(2)(g)(i)

Out of scope

4 At the roundtable, the companies wanted to know what success looked like for the PM at UNGA? We explained this was the ability to say in public that the Call countries had been working with industry to develop a structure to take the Call forward; that there had been progress on crisis response; that there was some agreement on a research agenda; s9(2)(ba)(i)
We were also clear that success for us was doing this in a collaborative fashion – that element should also be visible in New York. s6(a)

5 The roundtable focused, in large part, on the structural piece. We re-emphasised our view that reform of the GIFCT was the logical starting point for this conversation and that a reformed GIFCT would also advance the other outcomes in the Call. To do this would "require legwork" and time spent in co-design processes. The companies have agreed amongst themselves that the GIFCT does need to be a separate institution with its own staff and budget – but there are still significant questions to be resolved. These include the degree of independence, intersection with other international processes, location, and how a reshaped GIFCT can interact meaningfully with governments including in a crisis.

6 s9(2)(ba)(i)

s9(2)(ba)(i)

Crisis response protocol: 9 July workshop and next steps

8 Work on a crisis response protocol is a priority for the companies. s9(2)(b)(i)

9 s6(b)

10 s9(2)(j)

With support from post and the Global Security Fund, we (David Reid) hosted a workshop on 9 July in Paris on the crisis response protocol with attendees from supporter countries, civil society and law enforcement. The workshop covered a set of questions on how governments, civil society and media should engage with companies in an event like Christchurch, where a terrorist attack is combined with a significant online element.

11 These questions are being developed into a draft set of principles which will provide a point of engagement between supporter governments, civil society, academics and media on what to do in such a crisis. s9(2)(ba)(i)

12 As a follow-on from this work, New Zealand was invited to participate in a meeting of the EU Internet Forum on 16 July, which is also monitoring work by Europol to advance a crisis protocol, taking into account the principles being developed collaboratively with New Zealand. This was an opportunity to assess how the work underway there and among GIFCT members aligns with our thinking, and how we can ensure the pieces of work are complementary.

13 Our intention is to try convene a separate session on 23 July in Silicon Valley with companies and a wider group of countries to discuss how we can take our work forward and join up with the companies' product.

Civil society engagement

14 With support from Twitter, we also hosted a civil society event on the morning of 11 July. This was facilitated by Alex Stamos from Stanford University and included representatives from Microsoft, Twitter, Wikimedia, Moonshot CVE, Office of the UN High Commissioner for Human Rights, the American Civil Liberties Union, Storyful, UN Berkeley, the Electronic Frontier Foundation, Internet New Zealand, the UK, France, and Netsafe. Around 20 participants attended in person, with nine more dialling in.

15 The intent of the event was to discuss what commitments civil society might bring to the table in implementing the Call and how/where we might engage with groups over the coming months. The discussion was wide-ranging, with a number of issues raised but few solutions offered. Issues canvassed included:

- Questions about the problem the Call is intended to solve, including whether elimination of terrorist and violent extremist content is realistic and if the price of doing so is worth paying;
- The risks of not having a definition of "terrorist content" in the Call, given terrorism is an inherently political concept and whether the Call should be more focused on harm reduction;
- What the real issue had been with the Christchurch video and whether there was a market failure requiring intervention;
- The need to bring in voices from a wider array of civil society groups, including those in non-western countries;
- The need for civil society to be "earnestly" and actively engaged - but noting their limited capacity (essential functions should not be offloaded onto civil society) and the need to plan ahead;
- In designing a structure to take forward the Call, the construct should be broad to bring in a wide range of voices and all actors should be on an equal footing (civil society should not simply be an "add-on"); and
- The importance of transparency including by letting human rights and other groups in behind the scenes.

16 s9(2)(g)(i)

Models used by the International Criminal Court (ICC) include a tech advisory board and the appointment of two fellows, both of which provide a means for the ICC to reach out to the wider community. More broadly, however, it was clear there is no single place for coordination, knowledge-sharing and engagement on these issues. s9(2)(g)(i)

Other processes

17 The companies again emphasised their interest in continuing to work under the banner of the Call. s6(a)

18 s6(a)

Comment

19 s6(a); s9(2)(g)(i)

. However, while the roundtable was not the session we had expected to have, it was ultimately useful. And, in the discussions with s9(2)(ba)(i) , we were able to have the type of collaborative, engaged discussion that we were seeking on the detail of possible GIFCT organisational constructs. s9(2)(j)

20 Following the roundtable, s6(a) to us in the margins that it was the first time it has heard the companies collectively commit to GIFCT reform. We do now have time set aside for dedicated discussions on the structural question – the key will be ensuring these are genuinely ambitious co-design discussions and the final product includes an appropriate role for governments and civil society.

21 We have a week before the GIFCT conference and no shortage of preparation to do, including developing our "green lines" on our aspirations for a reshaped GIFCT s6(a) and preparation for discussions on the substance of a crisis response protocol.

ENDS

Revised Christchurch Call to Action: Annotated Version

Overview

We have drafted the Christchurch Call in a way that reflects certain key principles. These are:

- We support a free, open and secure internet. This is central to New Zealand's online policy, and is reflected at several points in the text;

- We want meaningful action on a narrow set of issues – that is, terrorist and violent extremist content online. We are not seeking to address a broader range of online harms in this text.

- We recognise that governments and companies have individual responsibilities, but that meaningful change requires collective action.

We have designed the Call to have two operational elements: that is, a **pledge** for all parties, committing to work to eliminate this content online, and a **series of commitments** intended to give effect to this pledge.

This is a non-binding political statement (i.e. not a treaty-level document). While we have aimed at developing commitments that, if given effect, will bring about change, the true value of the Call will be in its partners' willingness to adhere to and implement these commitments. We think there is willing from tech companies to take action, and we have tried to harness this here.

We expect partners to abide by these commitments, s9(2)(b)(ii)

The Call is currently drafted in such a way that the commitments are for governments and tech companies only. This is partly because, given the time available, we could not have a meaningful and credible negotiation with civil society – diverse as it is – on the content of the Call; nor does civil society have the same degree of agency over the commitments as companies or governments. Despite this, we plan to make it clear – both through our outreach and public communications – that we welcome support from civil society groups, both on and after 15 May. We have also discussed some of the key concepts in our engagement with civil society in San Francisco and Wellington.

Process

We received feedback on an initial draft of the text from the major tech companies and a number of the countries invited to the Call, s9(2)(ba)(i) In general, this feedback was constructive, and we have made a number of the changes to the text as a result. This included clarifying some of the commitments, revising others, and introducing a number of new ideas. Given the number of amendments, we have not tracked the changes into the Call below.

By the time of the summit in Paris, we expect each of the participating countries and companies to have provided a formal indication of their support for the text.s9(2)(b)(ii)

We issued this revised version of the Call to invitees on Tuesday 7 May. We are starting to receive some final comments on the text, many of which are cosmetic. s9(2)(b)(ii)

Call Text	Comment
The Christchurch Call to Action *To Eliminate Terrorist and Violent Extremist Content Online*	We have revisited this language and reverted to "eliminate".
A free, open and secure internet is a powerful tool by which to promote connectivity, enhance social inclusiveness and foster economic growth. The internet is, however, not immune from abuse by terrorist and violent extremist actors. This was tragically highlighted by the terrorist attacks of 15 March 2019 on the Muslim community of Christchurch – terror attacks that were designed to go viral. The dissemination of such content online has adverse impacts on our collective security and on people all over the world. Significant steps have already been taken to address this issue by, among others, the European Commission with initiatives such as the EU Internet Forum, the G20, and the G7, including work begun during France's G7 Presidency on combating the use of the internet for terrorist and violent extremist purposes, along with the Global Internet Forum to Counter Terrorism (GIFCT), the Global Counter Terrorism Forum, and the Aqaba process. The events of Christchurch highlighted once again the need for enhanced cooperation among the wide range of actors with influence over this issue, including governments, civil society, and	The **preamble** text is intended to set the context for this work, including in particular: • Grounding this in the experience of Christchurch, the uniqueness of the social media aspect, and the harm that this caused; • New Zealand's wider cyber security policy, which includes the promotion of a free, open and secure internet and recognition that human rights and international law apply online as they do offline; • the specific issue that we are trying to address in the wake of Christchurch (i.e. terrorist and violent extremist content) in order to carefully scope this work – the Call is not seeking to address all of the ills of the internet; • recognising work under way in other forums. s6(a) We want to acknowledge this work, while also recognising that more must be done; • our intended approach, which is to be collaborative.

online service providers, such as social media companies, to eliminate terrorist and violent extremist content online. The Call outlines collective, voluntary commitments from Governments and online service providers intended to address the issue of terrorist and violent extremist content online and to prevent the abuse of the internet as occurred in and after the Christchurch attacks. All action on this issue must be consistent with principles of a free, open and secure internet, without compromising human rights and fundamental freedoms, including freedom of expression. It must also recognise the internet's ability to act as a force for good, including by promoting innovation and economic development and fostering inclusive societies.	We have added some additional language to recognise the adverse impacts of the Christchurch video and to try anchor the Call's discussion in the specific harms that we saw following Christchurch. This is, in part, intended to address the fact that we are not defining "terrorist and violent extremist content" in the Call. s9(2)(ba)(i)
To that end, we, <u>the Governments</u>, commit 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.	We want tech companies to know this is a genuinely cooperative effort – we need to recognise the role governments play in addressing the drivers of violent extremism We have amended the language in this section to reflect suggestions from a number of counties, including emphasising "strengthening" rather than "building" resilience and inclusiveness and to show some of the ways in which this might be done.
Ensure the adoption and effective enforcement of applicable laws that prohibit the production or dissemination of terrorist and violent extremist content, in a manner consistent with human	This is intended to capture the criminalisation of terrorist and violent extremist content, at a domestic level – it addresses the individual element of the picture. In response to feedback, we gave

rights, including freedom of expression.	also added reference to the adoption of such laws.
Encourage media outlets to apply ethical rules when reporting on terrorist events, to avoid amplifying terrorist and violent extremist content.	s6(b) This is intended to encourage responsible reporting on terrorist events and content, in response to the publication by some media outlets of the video from the Christchurch attacker.

Have appropriate frameworks, such as broadcasting 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.	s9(2)(g)(i)
	s9(2)(j)

Consider appropriate action to prevent the use of online services to disseminate terrorist and violent extremist content, including through collaborative actions, such as: – Awareness-raising and capacity-building activities aimed at smaller online service providers; – Development of industry standards or voluntary frameworks; – Regulatory measures consistent with a free, open and secure internet and international human rights law.	s6(a) The new draft is intended to allow scope for consideration of a full range of regulatory-type measures, from voluntary frameworks through to black letter law. This framing means that we still acknowledge the importance of domestic regulation (as countries have, and will, regulate on this issue as well as alternative measures that could be designed in a collaborative way.

To that end, we, <u>the online service providers</u>, commit to:	Intended to go beyond social media platforms, to allow companies – large and small – with an online presence and role in content hosting to sign up to the Call.
Take transparent, specific measures to prevent the upload of terrorist and violent extremist content and to prevent the dissemination of this content, including by ensuring its immediate and permanent removal, in manner consistent with human rights and fundamental freedoms. Cooperative measures to achieve these outcomes may include technology development, the expansion and use of shared databases of hashes and URLs, and effective notice and takedown procedures.	s9(2)(ba)(i) We want the companies to demonstrate their commitment to action through being transparent about the measures they implement – i.e. outlining clearly the steps they are taking to action this commitment. s9(2)(ba)(i) s9(2)(ba)(i)
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	For clarity, we have split into two the commitment related to terms of service. This section is focused on transparency with respect to the companies' terms of service, which provides clarity for users and helps provide a framework for any limits on freedom of expression on the platforms.

detecting and removing terrorist and violent extremist content.	
Enforce those community standards or terms of service in a manner consistent with human rights and fundamental freedoms, including by: – Prioritising moderation of user-flagged terrorist and violent extremist content; – 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.	We have now clearly separated out the question of enforcement of community standards, and have highlighted what this might require. This includes appeal rights for users, which is important to mitigate the risk of any false positives (a risk flagged to us by civil society). s6(b)
Implement immediate, effective measures to mitigate the specific risk that terrorist and violent extremist content is disseminated through livestreaming, including identification of content for real-time review.	This proposal is largely unchanged - it gives scope to consider real-time moderation or limiting the availability of livestreaming. Google now only allows livestreaming on YouTube by verified users with at least 1,000 followers. s9(2)(g)(i)
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.	This is also largely unchanged - we want to ensure that the companies are making measurable progress against the goal of eliminating this content. Some companies already do this.
Review the operation of algorithms and other processes that may drive users towards and/or amplify terrorist and violent extremist content to better understand possible intervention points and to implement changes where this occurs. This may include using algorithms and other processes to redirect users	s9(2)(g)(i)

from such content or the promotion of credible, positive alternatives or counter-narratives. This may include building appropriate mechanisms for reporting, designed with local authorities.	s9(2)(j)
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.	This is a new commitment. s9(2)(ba)(i) we also want to see practical initiatives developed that can take forward the commitments in the Call.
<u>**To that end, we, Governments and online service providers, will work collectively to**</u>*:* **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.	Intended to acknowledge the joint responsibility we have to address violent extremism, and a role the platforms can have as a force for good. This has been reframed to emphasis working with civil society, who have particular expertise in this area.
Collaborate on the development of effective interventions, based on trusted information sharing about the effects of algorithmic and other processes, **to redirect users** from terrorist and violent extremist content.	This is a new commitment. It gets to the need for the companies to reconsider how their algorithms funnel users into terrorist content and to the role of governments in working with the companies on this, including through designing intervention points. There are models in the cyber security world for trusted information-sharing without risking trade secrets.
Accelerate collaborative 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.	This acknowledges the role both governments and companies have in supporting research; the focus on open source is intended to support the resilience and capacity of smaller platforms, and to make the work more naturally collaborative. It also now acknowledges the expertise in academia and elsewhere.

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.	This is a new commitment. It acknowledges the need for research on a number of fronts (e.g. to better understand right-wing extremism and how this manifests on the platforms through coded language, and to have better data on the harms caused by terrorist and violent extremist content more broadly)
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 accordance with rule of law and relevant human rights protections.	s6(a)
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.	This is a new commitment. It acknowledges the need for research on a number of fronts (e.g. to better understand right-wing extremism and how this manifests on the platforms through coded language, and to have better data on the harms caused by terrorist and violent extremist content more broadly)
Develop the capacity of smaller platforms 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.	We want to ensure that the Call does not only focus on the biggest platforms but provides tools (and the ability to sign up) for a range of much smaller platforms as well. s9(2)(j)
Collaborate, and support partner countries, in the development and implementation of best practice in preventing	s9(2)(ba)(i) It is intended to address the need to better work together on a range

the dissemination of terrorist and violent extremist content online, including through operational coordination and trusted information exchanges.	of fronts, including on policy development and options for information-sharing before a terrorist attack occurs.
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 accordance with relevant human rights protections.	s9(2)(ba)(i) This gets to the need to ensure that the companies and governments have arrangements in place to allow us to work effectively together in a crisis.
Protect and respect human rights, including by avoiding directly or indirectly contributing to adverse human rights impacts through business activities, and addressing such impacts where they occur.	This draws on the UN guiding principles on business and human rights and goes to the need for governments and companies to respect human rights in implementing the commitments in the Call. It also goes to the importance of ensuring that rights to be equal and free from discrimination are protected alongside freedom of expression.
Recognise the important role of civil society in supporting work on the issues and commitments in the Call, including through: – Offering expert advice on implementing the commitments in this Call in a manner consistent with a free, open and secure internet and with international human rights law; – Working, including with governments and online service providers, to increase transparency; – Where necessary, working to support users through company appeals and complaints processes.	This text is designed to acknowledge the important role of civil society on this issue – and the many fora at which civil society works on it – and provide a hook for their supporting/endorsing the Call. It will be not be possible to negotiate commitments from as diverse a group as "civil society" in the time available, but this offers an avenue for their participation. This section also highlights the need for strong civil society voices to support a free and open internet, to ensure companies and governments are not unreasonably restricting access to content.
Affirm our willingness to continue to work together, in existing	This reflects our desire to cascade the Call across a range of other

fora and relevant organizations, institutions, mechanisms and processes to assist one another and to build momentum and widen support for the Call.	meetings and fora, such as the G20, OECD and others – including a proposed event at Leader's Week in New York.
Will develop and support a range of practical, non-duplicative initiatives to ensure that this pledge is delivered.	Work to consider how the Call can be delivered will be done in the lead up to May 15 (e.g. in workshops with civil society) and beyond – we will complete work on how we take this work forward, especially with a view to a follow-up meeting at UNGA.
Acknowledge that governments, online service providers, and civil society may wish to take further cooperative action to address a broader range of harmful online content, such as the actions that will discussed further during the G7 Biarritz Summit, the G20, the Aqaba Process, the Five Country Ministerial, and a range of other fora.	s6(a) This is a nod to hate speech, disinformation and election interference, amongst other matters of concern.

NEW ZEALAND
FOREIGN AFFAIRS & TRADE

18 September 2019

Minister of Foreign Affairs		For action by	20 September 2019

The Christchurch Call: Progress Update

BRIEFING	General Purpose
PURPOSE	To provide a progress report on international work on the Christchurch Call to Action and on plans for a Call-centred side event in the margins of the United Nations General Assembly.

Recommended referrals

Prime Minister	For information by	20 September 2019
Minister for Greater Christchurch Regeneration	For information by	20 September 2019
Minister of Justice	For information by	20 September 2019
Minister for Trade and Export Growth	For information by	20 September 2019
Minister for Broadcasting, Communications and Digital Media	For information by	20 September 2019
Minister of Internal Affairs	For information by	20 September 2019

Contact details

NAME	ROLE	DIVISION	WORK PHONE	MOBILE PHONE
Pip McLachlan	Manager	Christchurch Call Team	s9(2)(a)	
Elizabeth Thomas	Policy Officer	Christchurch Call Team		

Minister's Office comments

The Christchurch Call: Progress Update

Key points

- Following the 15 May launch of the Christchurch Call to Action to eliminate terrorist and violent extremist content online, the Prime Minister and President Macron of France agreed to reconvene in the margins of the United Nations General Assembly (UNGA) on 23 September to take stock of progress.
- Since then, officials from the Ministry of Foreign Affairs and Trade and the Department of the Prime Minister and Cabinet have been working closely with the major US-based tech companies to take forward work in four priority areas.
- We have also been working with France to grow country support for the Call, and engaging with domestic and international civil society groups.
- An event has been scheduled for 23 September in the margins of UNGA Leaders' Week, co-hosted by the Prime Minister, HM King Abdullah II of Jordan and President Macron.
- We are on track to announce good progress at that event, including (this list is currently subject to an agreed embargo):
  - the launch of the Global Internet Forum to Counter Terrorism (GIFCT) as a standalone legal entity with dedicated resources to address the challenge of terrorist and violent extremist content on member company platforms;
  - a ready-to-deploy shared crisis protocol, outlining how companies and governments will engage in the event of a terrorist attack with an online component; and
  - at least 23 new country supporters for the Call.
- The announcements on GIFCT reform and crisis response are significant steps in preventing and responding to terrorist and violent extremist content online. This is a complex issue and an evolving threat – there is no quick fix.
- Work on algorithmic outcomes s9(2)(g)(i) and research will also be picked up under the new GIFCT structure.
- We see these outcomes as demonstrating what can be achieved through collaboration. s9(2)(j)

s9(2)(j)

- Some work on the Call will be ongoing including: participation in a new multi-stakeholder Independent Advisory Committee to the GIFCT; engagement with a new civil society Christchurch Call Advisory Network; participation at the Internet Governance Forum in November; engagement in an OECD work-stream on transparency reporting, co-funded by New Zealand; and a Google-led crisis response exercise in New Zealand in December.

Victoria Hallum
for Secretary of Foreign Affairs and Trade

Recommendations

It is recommended that you:

1 **Note** collaboration with the tech companies and a small group of countries has enabled progress under the Christchurch Call to Action since its launch on 15 May; Yes / ~~No~~

2 **Note** that Call supporting companies, countries and representatives from civil society will reconvene at an event on 23 September in the margins of the United Nations "Leaders' Week"; and Yes / ~~No~~

3 **Note** that at that event the Prime Minister will announce progress made under the Christchurch Call, including welcoming the proposal to reform the industry's Global Internet Forum to Counter Terrorism, launching a shared crisis response protocol and announcing a significant number of new Call-supporting countries. Yes / ~~No~~

Rt Hon Winston Peters
Minister of Foreign Affairs

Report

1. This report is an update on progress on international work on the Christchurch Call to Action to eliminate terrorist and violent extremist content online (the Christchurch Call) since its launch in Paris on 15 May.

2. It also provides an update on planning for an event on 23 September, in the margins of Leaders' Week, where leaders from Call supporting countries and tech companies will meet to take stock of progress and welcome new supporters.

Background

3. The Christchurch Call to Action to eliminate terrorist and violent extremist content online is at key element of New Zealand's international response to the Christchurch attacks – it seeks to respond to the harm caused by the livestream and viral distribution of the video of the attacks.

4. The Call was adopted at a high-level meeting in Paris on 15 May, co-hosted by Prime Minister Ardern and President Macron and attended by seven other leaders and eight major tech companies (including Twitter, Microsoft, Google/YouTube, Facebook and Amazon). Nine additional countries also came on board as founding supporters of the Call.[1] While the US did not join as a formal supporter, it issued a statement that was supportive in substance.

5. Following the Paris meeting, s9(2)(ba)(i) four priority areas for action were identified:
   - reform of an existing industry body (the Global Internet Forum to Counter Terrorism (GFICT)) to be more inclusive and effective, and take forward Call-related work;
   - developing a shared crisis response protocol to enable countries and companies to work together better in future attacks;
   - better understanding where there are gaps in the research on terrorist and violent extremist content online; and
   - better understanding how companies' algorithms can drive users to more extreme content, and identifying intervention points.

6. At the conclusion of the 15 May meeting, the Prime Minister and President Macron undertook to regroup with Call supporters on the margins of UNGA Leaders' Week, to assess progress against the Call.

7. To make meaningful progress by September, our efforts have coalesced across three broad workstreams: engagement with companies; engagement with

[1] Countries supporting the Call on 15 May were: Australia; Canada; European Commission; France; Germany; Indonesia; India; Ireland; Italy; Japan; Jordan; The Netherlands; New Zealand; Norway; Senegal; Spain; Sweden; United Kingdom

countries; and engagement with civil society. This work has been led by the Ministry, with expert input from the Department of the Prime Minister and Cabinet.

Company engagement

8. s9(2)(j)

9. We are on track to collectively announce good progress, including:

   - The **launch of the GIFCT as a standalone legal entity** with an executive director, dedicated staffing and resources. It will also have a new governance structure, including an independent advisory committee, comprised of civil society and government representatives. s9(2)(j)
   s9(2)(j)
   - A **ready-to-deploy shared crisis protocol**, outlining how companies and governments will cooperate and respond in the event of a terrorist attack with an online component. GIFCT companies have developed a complementary 'content incident protocol' to guide their internal response to real-world crises. We are asking supporter companies and countries to endorse the protocol as something they are prepared to use.
   - A **gap analysis on research** on issues related to the Call, intended to help better target future funding and highlight where more data is needed.
   - The establishment of a multi-stakeholder working group in the new GIFCT focused on better understanding how **algorithms** may affect user engagement with terrorist and violent extremist content. s9(2)(g)(i)
   s9(2)(g)(i)

10 s9(2)(g)(i)

UNGA: Key programme elements

Leaders' Dialogue

11. The centrepiece for the Call-related elements at UNGA will be an event in the early evening of 23 September, co-hosted by Prime Minister Ardern, President Macron of France (to be confirmed), and His Majesty King Abdullah II of Jordan.

12. This event has been styled as a "Leaders' Dialogue" on strategic responses to eliminating terrorist and violent extremist content online. It is an invitation-only event, with speaking slots reserved for Heads of State/Government. A representative of Secretary-General Guterres and King Abdullah will open, speaking to UN counter-terrorism efforts and the Aqaba Process respectively, but

the bulk of the event will then focus on the Christchurch Call. Speaking times are limited but, as in Paris, sufficient to provide countries, companies, and civil society with an opportunity to highlight their perspectives on the Call and efforts to implement it.

13. We are still receiving RSVPs for the event but so far around 20 leaders are confirmed to attend, along with Facebook Chief Operating Officer Sheryl Sandberg, Microsoft President and Chief Legal Officer Brad Smith, and Google/YouTube's Senior Vice President for Global Affairs, Kent Walker.

14. We anticipate that the event closed to media but a press conference will follow, providing an opportunity for the Prime Minister to publicly announce progress made under the Call – including GIFCT reform, the shared crisis response protocol and the list of new supporters (discussed below). s9(2)(j)
s9(2)(j)

s9(2)(j) but New Zealand and France will release a joint press release and the GIFCT companies a blog post.

Tech company roundtable

15. In Paris, the Prime Minister and the King of Jordan hosted a roundtable discussion with the tech companies on 15 May. This was an opportunity for the Prime Minister to have a substantive conversation with senior representatives from the tech companies on next steps to implement the Call, and has shaped the subsequent work programme.

16. We will hold a follow-up roundtable with the Prime Minister and the GIFCT founding companies in the evening of 23 September. The objectives are:

- To provide an opportunity for substantive engagement on progress with the tech companies, outside of the UN context.
- To discuss next steps on the Christchurch Call and opportunities to take forward some of the other key commitments.
- To provide an opportunity for the tech companies to speak to their individual progress against the Call and where there is scope for ongoing collaboration.
- To highlight the collaborative nature of the Christchurch Call through engagement with tech companies and civil society.

17. The first part of the roundtable will be a closed-door conversation on next steps under the Call. For the final portion, we will include members of the Advisory Network for a more open discussion.

Country engagement

18. Country engagement has been our second key workstream ahead of the UNGA events described above. Our focus on country supporters has had two strands:

engagement with 'foundational supporters' (i.e. those that supported the Call on 15 May); and working with France to deliver a 'second wave' of new country supporters, to be announced and profiled on 23 September.

19. Since May, we have had particularly close engagement with France, the UK, Canada and the US (despite the latter not having joined the Call as an official supporter). s6(b)
s6(b) We have also worked closely with Norway and the EU on crisis response, among others.

20. s9(2)(ba)(i)

21. s9(2)(ba)(i)

22. s6(b)
s6(b)
s6(a); s6(b) 6(a), s6(b)

New supporters

23. Shortly after Paris, we agreed with France that we would target a 'second wave' of country supporters for the Call, to be announced as part of a wider sign of progress at UNGA. We have developed a list of target countries with France – primarily members of the Freedom Online Coalition[2], plus members of the European Union s6(b) Posts are in the process of conducting joint demarches with France and, at this stage, we expect to be able to announce at least 23 new supporters from a wide geographic spread.[3] This list is also currently subject to an embargo.

[2] A group of 30 governments committed to protecting and promoting online freedoms domestically and abroad.

[3] New supporters at time of writing: Argentina, Belgium, Bulgaria, Chile, Colombia, Cyprus, Denmark, Finland, Hungary, Kenya, Latvia, Lithuania, Luxembourg, Maldives, Malta, Mexico, Mongolia, Poland,

24. s6(b)

Civil society engagement

25. At the Voices for Action civil society event in Paris, we committed to engage with civil society as we worked to implement the Call. Supported by s9(2)(ba)(i) s9(2)(ba)(i) this has been a core part of our work since May, including by providing regular updates and opportunities to comment to a global network of civil society organisations. This group includes civil liberties and human rights groups, academics and researchers, counter-terrorism and countering violent extremism experts, and the technical internet community.

26. This has provided us with a channel to hear civil society concerns and to draw on a range of expertise. The shared crisis protocol, for instance, has been refined and developed through a multi-stakeholder process. Throughout, it has been important for us to emphasise the Call's focus on protecting human rights and fundamental freedoms – and to emphasise what made the Christchurch attacks different, requiring a global response.

27. Civil society groups have repeatedly emphasised the importance of transparency and of having civil society in the room as a significant stakeholder. We have therefore made space at the UNGA event for ten civil society representatives, including three speaking slots. These will be filled by members of the newly established Christchurch Call Advisory Network. The Advisory Network provides individuals and organisations with an interest and expertise in issues with a formal relationship to the Call (they will be listed on the website) and the opportunity to attend the UNGA event. s6(b) s6(b) likely including a Call-focused side event at the Internet Governance Forum meeting in Berlin in November.

Out of scope

The Christchurch Call: Progress Update

Out of scope

NEW ZEALAND
FOREIGN AFFAIRS & TRADE

21 November 2019

Minister of Foreign Affairs	For action by	28 November 2019

The Christchurch Call: Shared Crisis Response Protocol Workshop

BRIEFING General Purpose

PURPOSE To provide an overview of the online incident response workshop being hosted by YouTube/Google in Wellington, 3-4 December, in response to the Christchurch Call to Action.

Recommended referrals

Prime Minister	For information by	28 November 2019
Minister of Justice	For information by	28 November 2019
Minister for Trade and Export Growth	For information by	28 November 2019
Minister of Police	For information by	28 November 2019
Minister of Broadcasting, Communications and Digital Media	For information by	28 November 2019
Minister of Internal Affairs	For information by	28 November 2019

Contact details

NAME	ROLE	DIVISION	WORK PHONE
Pip McLachlan	Manager	Christchurch Call Team	s9(2)(a)
Carolyn Wilson	Senior Policy Officer	Christchurch Call Team	

Minister's Office comments

Key points

- YouTube/Google is hosting an online incident response workshop in Wellington, 3-4 December. The Prime Minister will make opening remarks.
- The workshop will be an international, multi-stakeholder event with representation from country and tech company supporters of the Christchurch Call to Action to eliminate terrorist and violent extremist content online, as well as members of civil society and non-government organisations (both domestic and international).
- The workshop will test and refine the Christchurch Call shared crisis response protocol developed by New Zealand with other Call supporters, with input from civil society. This protocol was part of a commitment made by governments and online service providers in the Call, to "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."
- s6(a)
- The workshop will be closed to media, but the opening remarks – delivered by Prime Minister Jacinda Ardern and Gautam Anand, Head Senior Director for YouTube for Partnership and Operations, Asia Pacific – will be open to media.

Victoria Hallum
for Secretary of Foreign Affairs and Trade

Recommendations

It is recommended that you:

1 **Note** that an online incident response workshop will be convened and funded by YouTube/Google in Wellington, 3-4 December; **Yes / ~~No~~**

2 **Note** that the Prime Minister will be making opening remarks; **Yes / ~~No~~**

3 **Note** that this workshop will be an opportunity to test and refine the Christchurch Call shared crisis response protocol, designed as part of the Christchurch Call to Action; **Yes / ~~No~~**

4 **Note** that participants include working level representatives from technology companies, government officials from Call-supporting countries, civil society and non-government organisations. **Yes / ~~No~~**

5 s9(2)(ba)(i) **Yes / ~~No~~**

Winston Peters

Rt Hon Winston Peters
Minister of Foreign Affairs

Report

1. As part of the Christchurch Call to Action to eliminate terrorist and violent extremist content online, governments and online service providers made a commitment to "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."

2. Pursuant to this commitment, New Zealand led the development of a **shared crisis response protocol.** This was developed through discussions with Call-supporting countries and tech companies, plus relevant civil society and non-government representatives. The protocol was announced by the Prime Minister on 23 September, at a series of events during UNGA Leaders' Week that took stock of progress made around the Call since May.

3. The protocol is operationally ready, and able to be activated if an event like the Christchurch attack were to happen again. The intention is to be able to react quickly, effectively and in a coordinated manner with Call supporting governments and tech companies, to the dissemination of terrorist and violent extremist content online following such an attack. The protocol establishes common thresholds for action, standards of performance and transparency, and a common decision-making framework for companies that are part of the Global Internet Forum to Counter Terrorism (GIFCT) on how they would manage content on their platforms.

4. s6(b)

5. The protocol is not set in stone – it has always been pitched as a living document, to be refined based on real world lessons. It complements other initiatives. These include:

   - A **Content Incident Protocol**, developed by and for GIFCT companies, which creates an action plan for its member companies when faced with attacks coordinated with the specific and planned intent of content going viral. s9(2)(b)(i)

s9(2)(b)(i)

   The CIP applies to GIFCT member companies only; it interacts with the Crisis Response Protocol when the latter is activated to ensure effective coordination between companies and countries.

- The European Union's Response Protocol to Online Crisis Stemming from Terrorist and Violent Extremist Attacks (**EU Crisis Protocol**), which is a voluntary mechanism to help coordinate a rapid, collective and cross-border response to the viral spread of TVEC online. This protocol is for EU member states, Europol and online service providers only.

6. Sitting alongside these is New Zealand's domestic crisis response process. This is in development through the Department of Internal Affairs. This process brings together government, industry and non-governmental actors within New Zealand to coordinate efforts to respond a to a major online safety event such as occurred following the Christchurch attacks.

7. s6(a)

8. Against this context, the Government has welcomed YouTube/Google's initiative to host a workshop in Wellington, 3-4 December. Our core objectives for this workshop are as follows:

   - To test the Christchurch Call shared crisis response protocol in a multi-stakeholder format, i.e., with representatives from countries, tech companies, civil society and non-governmental organisations;
   - To engage with these stakeholders from the Christchurch Call community on how the shared crisis response protocol works and interacts with other protocols and evolving risks;
   - To inform the future agenda of the GIFCT's proposed crisis response working group that will be established as part of the GIFCT's new structure;
   - To provide a public profile of the value of collaboration around online incident response, as it pertains to terrorist and violent extremist content.

9. The outcomes we seek to achieve as a direct result of the workshop include:

   - Increased understanding of roles and responsibilities;
   - Increased collective understanding and better evaluation of threat, potential human rights impacts, notifications, alerts and information sharing processes between government and industry;
   - Clearer expectations of response and communications between countries and companies responding to these events;
   - Strengthened relationships between key stakeholders within the international Call community (i.e. governments, online service providers, civil society and non-government organisations).

10. The event is being facilitated by the Atlantic Council – a U.S based international affairs think-tank, with experience facilitating events concerning cybersecurity and counter-terrorism/violent extremism.

11. The two-day workshop will have the following components:

    - An opening address by the Prime Minister, introduced by Gautam Anand, Head Senior Director for YouTube for Partnership and Operations, Asia Pacific;

    - Two panel discussions: one on the role of traditional media and protecting human rights in the context of online crisis response; another on preparing for the evolving threat landscape;

    - Up to three scenarios, facilitated by Atlantic Council, that will test the dimensions of the shared crisis response protocol including its practicality and legitimacy as a tool for key stakeholders, as well as wider human rights implications i.e. transparency, online freedoms, the dangers of misuse and the integrity of the internet.

12. There will be around 90 participants at the workshop, including:

    - Officials from, Germany, Australia, Canada, the European Commission, France, Germany, Japan, Jordan and the European Union, the UK and US;

    - Counter-terrorism and policy experts from Facebook, YouTube, Google, Amazon, Microsoft, Twitter and Tech Against Terrorism[1] (which focusses on engagement with smaller platforms);

    - Civil society and non-government organisation representatives (domestic and international), including members of Google's 'Trusted Flagger' network, plus some members of the Advisory Network to the Christchurch Call.

13. As well as being an opportunity to strengthen the shared crisis response protocol, we expect this workshop will provide useful and timely input into the proposed GIFCT crisis response working group, which New Zealand has proposed as an early deliverable for the restructured entity, as launched by companies on 23 September.

Communications

14. This is not a public-facing event. The Prime Minister's opening remarks, delivered alongside Gautam Anand, will be open to media. But the workshop, including panel discussions and all supporting written material, will be held "in-confidence". This is due to security considerations and to ensure free and frank participation.

15. Public communications generated after the event may include a joint high-level PR between the Prime Minister and Google, an independent statement from the GIFCT and additional commentary from Google.

[1] Tech Against Terrorism is an initiative launched and supported by the United Nations Counter Terrorism Executive Directorate (UN CTED) working with the global tech industry to tackle terrorist use of the internet whilst respecting human rights.