DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Proactive Release

The following documents have been proactively released by the Department of the Prime Minister and Cabinet (DPMC) on behalf of Rt Hon Chris Hipkins, Prime Minister:

Proactive Release: Update on the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online

The following documents have been included in this release:

Title of paper: Update on the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online (CAB-23-SUB-0338 refers)

Title of minute: Report of the Cabinet Social Wellbeing Committee: Period Ended 28 July 2023 (CAB-23-MIN-0338 refers)

Title of minute: Update on the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online (SWC-23-MIN-0098 refers)

Some parts of this information release would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant section of the Act that would apply has been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Key to redaction codes:

- Section 6(a), making available the information would be likely to prejudice the security of New Zealand or the international relations of the Government of New Zealand.
- Section 9(2)(f)(iv), maintain the constitutional conventions for the time being which protect the confidentiality of advice tendered by Ministers of the Crown and officials.
- section 9(2)(g)(i), to maintain the effective conduct of public affairs through the free and frank expression of opinion.
- Section 9(2)(j), to enable negotiations to be carried on without prejudice or disadvantage.

Office of the Prime Minister

Cabinet Social Wellbeing Committee

Update on the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online

Proposal

1 This paper provides an update on the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online ("the Call") and sets out the next steps in its work.

Relation to Government priorities

2 The Christchurch Call was established in 2019 as part of the response to the March 15 terrorist attack and is one of the Government's top international policy priorities.

3 Although a separate stream of work, the Government's response to the Royal Commission of Inquiry into the attack on Christchurch Masjidain covers some related issues and has led to work relevant to the fulfilment of New Zealand's commitments under the Call.

Executive Summary

4 The Call has achieved substantial positive progress in eliminating terrorist and violent extremist content (TVEC) from social media platforms, leading to improved crisis response systems, and fostering a global effort supported by dedicated structures and resources to stay ahead of terrorist and online extremist threats. In line with the direction from Call Leaders in 2022, its major focus is now on mitigating radicalisation of at-risk users towards violence, supporting the safe deployment of new technologies, and engaging young people in its work. The Call model involves concerted multistakeholder collaboration between governments, researchers, regulators, industry, and impacted communities, including to manage the risks and realise the positive potential of artificial intelligence (AI). The Call is at the forefront of developing tools that will assist with ongoing work to prevent production and distribution of TVEC, and which have important applications well beyond it.

Background

5 The March 15 Terrorist attack was a dark day for New Zealand, with 51 members of our Muslim Community murdered while at worship. The attack was pre-planned as a propaganda event to draw attention to white identity conspiracy theories. This strategy engaged an extremist online community that celebrated previous white supremacist attacks including the 2011 attack on Utøya island and Oslo. The livestream of the March 15 attack featured graphic footage of murder, viewed through the perspective of the terrorist, and was accompanied by a 74-page manifesto outlining his purpose, methods, and a blueprint for anyone wishing to follow in his footsteps.

6 Content from March 15 was spread widely online. Only around 4,000 people saw the initial live stream on Facebook, but millions of copies and iterations were generated by

others seeking to evade the online safety tools and exploit the algorithmic distribution systems on mainstream platforms. Facebook removed 1.5 million copies from its services in the first 24 hours. YouTube saw a new attempt to upload the video each second over the first 48 hours following the attack. Copies of the video were widespread on ordinary newsfeeds on Twitter and other large platforms for a considerable period of time following the attack. The enormous scale of the distribution of the attack video helped bring home to the platforms the need for urgent change to their systems.

7 Members of the Christchurch Muslim Community reported the trauma they experienced from seeing the footage. For many of them it was their last glimpse of their loved ones alive. Some who saw the footage appear repeatedly on their feeds have said that they are unable to let go of the imagery and the fear and pain it caused. More generally, mental health helplines in New Zealand reported a significant number of calls relating to the content in the immediate aftermath of the attack.

8 There have been numerous attempts by other attackers to replicate these methods or outdo what happened in Christchurch. Online extremist communities have canonised the Christchurch terrorist as a "Saint", alongside previous perpetrators of similar attacks. Many terrorists cite their engagement with extremist communities and content online as a significant factor in their own radicalisation to violence, and a source of information to adapt their methods and tactics. In El Paso, Poway, Halle, Bratislava, and Buffalo among other attacks, terrorists have cited the Christchurch manifesto and the actions of the perpetrator as part of their motivation.

9 Content has also been used in re-victimisation. Versions of the livestream have been edited with the addition of a 'kill count' and other features designed to trivialise the act and dehumanise the victims and survivors, converted into video games, cartoons, and memes and disseminated through gaming platforms and blogs. Footage of Christchurch has been mixed with content from more recent attacks and sent directly to survivors of March 15. Video 'documentaries' using the content have also been produced, claiming that the attack was a 'false flag' intended to create the case for gun law changes.

The Christchurch Call

10 The Christchurch Call was part of the response to the March 15 attacks. The Government was concerned to address the presenting issue of terrorist content online in a way that reflected our values and the global nature of the internet, and to create enduring solutions, that prevent platforms from being weaponised.

11 The process of developing the Call involved direct negotiations with online service providers and governments, and experts in civil society and academia. The Call contains 25 specific commitments detailing how governments and the major tech platforms would act to eliminate TVEC online, and an overarching commitment to promote human rights and a free, open, secure internet.

12 The Call was launched on 15 May 2019 in Paris at a Summit co-chaired by President Macron and former Prime Minister Ardern. As well as other world leaders, attendees included tech company executives and representatives of civil society organisations. President Macron of France and his team were instrumental in arrangements,

leveraging their existing work on technology and G7 Presidency to help create a stand-alone Call Summit.

The Call has made a substantive difference

13 Since its launch, the Call has galvanised significant change.

13.1 The major tech platforms took immediate actions, including updating their terms of use, improving user reporting, enhancing technology to spot TVEC, including digital fingerprinting and artificial intelligence (AI) tools, controls on livestreaming, and regular transparency reports with information about how terrorist content is identified and removed. The livestreaming controls have stopped multiple attackers from achieving their desired impact.

13.2 New Zealand spearheaded multistakeholder negotiations on a new shared crisis response system. This system now delivers coordination between online service providers and other interested parties during a terrorist or violent extremist incident, to ensure viral content is addressed in a more timely, coordinated, and effective manner. It provides oversight and improved debriefing with civil society and government stakeholders. As at the beginning of 2023, the crisis response system had been used 306 times to monitor and assess incidents in 44 countries. On seven occasions the system responded to non-video content (2021 in Kunduz, Kabul, and Amsterdam and 2022 in Udaipur, Colleyville, Bratislava, and Washington DC) and on four occasions the system enabled coordinated takedown of livestream or video content by the major platforms (Halle, Germany October 2022, Glendale Arizona May 2020, Buffalo, USA May 2022, and Memphis USA September 2022).

13.3 New Zealand initiated a multistakeholder process to shift the Global Internet Forum to Counter Terrorism (GIFCT) from an industry body to a non-governmental organisation, with funding from the technology sector, staff, and a mandate to develop shared capabilities and knowledge for the sector.

The GIFCT:

(a) commissions insights from independent experts about the evolving tactics, capabilities, and identities of violent extremist groups and shares them widely;

(b) maintains and manages access to a database of 'hash' identifiers used to find known terrorist and violent extremist content and remove it from platforms;

(c) works with 'Tech Against Terrorism' (a UN-affiliated tech non-profit) to mentor companies, help them develop appropriate policies and deploy technology to counteract terrorist and violent extremist use of their platforms;

(d) holds workshops and outreach with social scientists and extremism experts to build capability and expertise on addressing TVEC;

(e) commissions the development of new tools such as automated classifiers for audio content;

(f) convenes multistakeholder working groups, including on incident response, transparency, and legal frameworks.

13.4 The Call Community has expanded significantly from the initial 18 supporters, and now includes:

(a) 55 Governments, plus the European Commission, representing virtually all of the world's liberal democracies that support a free, open, and secure internet;

(b) 14 online service providers: Amazon, Meta, Google, YouTube, Zoom, DailyMotion, Microsoft, Qwant, JeuxVideo, Line, Twitter, Roblox, Mega, and Clubhouse, with a onboarding of further supporters expected in coming months;

(c) an independent advisory network of more than 50 civil society, human rights, and digital rights experts, representatives of affected communities, experts on extremism and radicalisation, technical and internet governance experts, civil rights and free speech advocacy organisations, journalists, consumer safety organisations and policy think tanks; and

(d) a new category of 'partner organisations' that bring specific expertise: The Global Community Engagement and Resilience Fund, Tech Against Terrorism, the Council of Europe (a regional human rights body), and the UN Economic Scientific and Cultural Organisation.

(e) There is a substantial pipeline of new online service providers, civil society organisations and prospective partner organisations working their way through the Call's multistakeholder onboarding process.

14 In addition to the issue of TVEC distribution, the Call requires governments and tech firms to work on the underlying drivers and risk factors that contribute to people being radicalised to violence. Radicalisation is a complex phenomenon with many offline contributing factors. However many violent extremists highlight that they were radicalised online. Call supporters have commissioned and shared extensive research, rolled out positive intervention and redirection programmes, and made changes to their algorithmic ranking systems in efforts to reduce the contribution of online platforms to this process.

15 In September 2022, New Zealand, the USA, Microsoft, Twitter, and a non-profit organisation called OpenMined launched the Christchurch Call Initiative on Algorithmic Outcomes (CCIAO). In their first joint project under CCIAO, New Zealand and the other supporters are developing and testing new tools that allow researchers to study the outcomes of algorithmic processes in a safe and secure way, with a focus on algorithmic systems that determine the content people see on their feeds on the major social media platforms. This project is in its early stages but is going well. It has verified and completed a proof of function test, working with major social media platforms. This tool will simplify the testing needed to understand the user journeys of at-risk people, and to test whether interventions to disrupt radicalisation can be made more effective.

There are some risks to Call progress

16 The Call places significant demands on supporters and other members of the Call Community. It does so against a backdrop of economic, geopolitical, and regulatory competition, pressure on revenues in the sector, and many organisations seeking to carve out a role in the digital landscape, particularly internationally.

17 It has been challenging to find ways of effectively studying algorithmic outcomes and the impact of online user journeys on radicalisation to violence. Such studies typically require access to sensitive datasets and encounter legal barriers and raise ethical and practical issues. Substantial efforts have been made by social media companies to improve their algorithmic recommendation systems but, without independent study, it is difficult to understand the impacts of these changes. The EU's new Digital Services Act creates a legal framework for researcher access to data but delivering this in a manner consistent with existing privacy frameworks is still to be worked through by authorities. The CCIAO is an important response to this challenge, and over time should create significant opportunities for improved access to information, as well as a safer environment for users.

18 The economic environment for big tech platforms has changed in recent times. This has led to significant industry layoffs and pressure on resources for new initiatives. As part of this streamlining effort firms have indicated that AI tools will play a greater role in their trust and safety efforts. As such the CCIAO and related work on AI safety will play an increasingly important role in the Call work.

19 The regulatory environment is also changing rapidly, and this consumes significant resources for the Call's stakeholders. The EU's Digital Services Act applies a risk-based framework to regulation of large digital platforms and requires external risk assessment and audit. This may be helpful for progressing the Call, particularly if protocols and tools developed by the Call Community can be acknowledged as appropriate risk mitigations for the purposes of the Act. Regulatory efforts in the United States, India, and elsewhere will also have impacts on our work, and ensuring that responses are consistent and effective at a global level remains an important objective for the Call Community.

20 GIFCT 9(2)(g)(i), 9(2)(j) It has been successful in setting up a system to rapidly identify TVEC in video and photo format during an incident, and in commissioning research that it shares with its members. Its mentoring programme, delivered by Tech Against Terrorism, has helped lift performance across the whole sector. 9(2)(g)(i), 9(2)(j)
9(2)(g)(i), 9(2)(j)
New Zealand has sought to facilitate dialogue with Call leaders and with GIFCT 9(2)(g)(i), 9(2)(j)

21 The Christchurch Call's Civil Society Advisory Network (CCAN) operates on a voluntary basis, with support provided by New Zealand and France for a part-time administrator to assist with coordination. Its membership includes individual experts, and small, medium, and large organisations operating in different time zones, with widely varying interest areas and priorities. Inevitably, it can be challenging to build a sufficient level of trust such that individuals can develop and share advice, including where there are divergent perspectives on an issue. Obtaining CCAN's advice and input requires time and attention, in an environment where both the technologies deployed online, and the strategies of violent extremists, evolve quickly. Involving CCAN closely in our work remains a priority and is essential to the success of the Call. Regular outreach by New Zealand and France with CCAN members is important. A shared Community platform is also being scoped as a means of facilitating greater participation and information sharing by the Call community, including its civil society members.

Next steps for the Call

22 At the most recent Call Leaders' Summit, in September 2022, Rt Hon Ardern and President Macron issued a joint co-Chairs statement, endorsed by the Leaders present, setting out priorities for the next stages of Call work.

This included:

(a) Sharpening incident response, and measures to address the proliferation of content online through: developing and making available leading edge technological tools; outreach to small firms and expansion of the support base; developing options for addressing the impact of unmoderated and 'alt-tech' services, and continued efforts to test and refine the shared incident protocol;

(b) Providing a better evidence base about radicalisation to violence through: promoting targeted research pilots, making use of new tools such as those developed by the CCIAO, promoting a wide range of tools including third party standards and quality metrics to promote user choice and responsibility to help disrupt TVEC, and investigating the linkages between gender-based violence and radicalisation.

(c) Future proofing the Call by supporting the adoption of new technologies while promoting safety and security against TVEC; increasing our understanding of the challenges and opportunities from new technologies; and engaging with young people across our work programme.

23 In March this year, I appointed Rt Hon Jacinda Ardern as my Special Envoy for the Christchurch Call. Rt Hon Ardern will engage on my behalf with Heads of State and Government, and leaders from civil society, industry, and international institutions to advance the Call. Her experience and status as a former head of Government ensures that she can lead outreach on my behalf and maintain the Call as a leader-level initiative.

24 The Special Envoy works with the Christchurch Call Unit – a joint venture of DPMC and MFAT to accelerate the delivery of Call outcomes, mobilise additional long-term support and funding for the Call, build capability on digital policy issues within the

public service, and enhance New Zealand's leadership role on technology issues internationally.

25 AI plays a significant role in identifying and removing TVEC and managing the user environment to address the risk of radicalisation to violence. New, more powerful AI opens the way for scalable interventions at a lower cost, but also comes with risks of exploitation and misuse. The CCIAO will open new means of studying AI/user interactions, measuring the effectiveness of safety features and interventions, and providing the community with a means of understanding how users are impacted by the widespread deployment of AI tools including generative AI.

26 The Call community does important work on AI where it relates to TVEC. There has also been considerable and growing interest from the tech sector, from experts and from governments in how a similar values-based multistakeholder leadership model could be applied to the broader question of AI risk and governance. 9(2)(j) 9(2)(j)

27 The Special Envoy's upcoming fellowships at Harvard University provide an opportunity to expand the resources and institutions available to support the Call's priority outputs.

28 6(a), 9(2)(f)(iv) There has been significant positive outreach from Leaders seeking to make a positive contribution to the work of the Call. This bodes well for the Call sustaining itself into the future.

Closer to home: New Zealand has responsibilities as a Call Supporter

29 In addition to our responsibilities as co-founders and stewards of the Call internationally, New Zealand has commitments as an individual Government supporter to: counter the drivers of violent extremism; strengthen social resilience and inclusion; fight inequality; strengthen media literacy in education; facilitate voluntary frameworks or standards for responsible reporting on terrorism and violent extremism; and effectively enforce laws that prohibit TVEC.

30 New Zealand has undertaken through the Call to uphold international human rights law and a free, open secure internet. Among other things, this requires New Zealand to consider relevant domestic legislation and our engagement in international internet governance institutions and digital initiatives in light of these commitments.

31 New Zealand can uphold its commitments by:

(a) Supporting the multistakeholder model for internet governance and contributing to global governance institutions such as the Internet Corporation for Assigned Names and Numbers, the International Telecommunications Union, the UN

Internet Governance Forum, as well as initiatives such as the Freedom Online Coalition that defend and promote human rights online;

(b) Looking for international multistakeholder approaches to address problems that arise online, or where appropriate finding approaches to regulation or governance that can accommodate international harmonised standards or frameworks;

(c) In the context of national legislation, assessing the potential impact on a free, open, secure internet and human rights online. The Call Unit has helped provide input for example on the Safer Online Platforms and Media Platforms Review, the implementation of Recommendation 12 of the Royal Commission of Inquiry, and the development of a domestic crisis response protocol and transparency framework for Government content takedown requests; and

(d) Continuing to advance the Call in such a way that impacted communities, industry, government, and civil society all contribute to the common objective of eliminating TVEC online.

Human Rights

32 The Christchurch Call requires supporters including the New Zealand Government, other Governments and Online Service Providers to carry out their work through actions consistent with international human rights law and human rights responsibilities applying to business. There are numerous human rights organisations and experts engaged in the Call Community. The GIFCT commissions regular external human rights impact assessments of its work, and many of the Call's industry supporters have assessment frameworks in place.

33 Our experience shows that implementing commitments in a human rights-consistent manner can be a complex task. It requires that organisations protect and respect human rights, reconciling rights that can sometimes appear to be in conflict, apply judgement, and subject that judgement to scrutiny. The activities of human users, law enforcement and security agencies, and machine learning systems for curation of the online experience, all play into a complex landscape in which the responsibility for adverse human rights impacts can go in multiple directions.

34 Ensuring human rights impacts are properly managed requires ongoing dialogue in a multistakeholder setting in which rights advocates and communities impacted by terrorism and violent extremism can participate effectively. This also includes addressing gender-based violence as a feature of radicalising narratives – something Leaders have asked the Call community to prioritise over the coming period. The Christchurch Call provides a unique platform for those conversations.

Consultation

35 The following agencies and organisations were consulted on this paper: Ministry of Foreign Affairs and Trade, Department of Internal Affairs, Ministry for Ethnic Communities, Ministry for Women, Ministry of Business Innovation and Employment, Ministry of Justice, Statistics NZ, Te Mana Whakaatu – Classification Office, and NZ Police. The Department of the Prime Minister and Cabinet (PAG) was informed.

36 MBIE, DIA, and Statistics NZ pointed to their work to understand how AI can be safely and responsibly deployed in Aotearoa in a way that promotes economic and other opportunities. Future work may include development of a cross-agency work programme spanning AI in the public sector and wider economy. The Call Unit in DPMC, MBIE, DIA and Statistics NZ regularly share information and updates on related work.

Proactive Release

37 This paper will be proactively released with appropriate redactions in accordance with Cabinet Guidelines.

Recommendations

The Prime Minister recommends that the Committee:

1 note that the Christchurch Call, launched in May 2019 forms part of the Government's policy response to the March 15 terror attack and has achieved positive change in the way online service providers, governments, and civil society act to eliminate terrorist and violent extremist content online.

2 note that, as liberal democracies seek ways to manage the risks and opportunities of technologies such as artificial intelligence, our co-leadership of the Call (alongside France) has delivered valuable experience in the development of multistakeholder solutions and highly relevant work on the impacts of algorithmic processes.

3 note that the Call has an ambitious work programme and faces some challenges to delivery and that my appointment of a Special Envoy will help us to advance this work, and manage any risks, whilst maintaining the profile of the Call as a leading international tech initiative.

4 invite the Prime Minister, to provide a further update on progress 6(a), 9(2)(f)(iv)

Authorised for lodgement

Rt Hon Chris Hipkins

Prime Minister

Glossary of Terms

AI (Artificial Intelligence): the science of making machines that combine computer systems and datasets to enable problem solving.

Algorithm: a set of instructions designed to perform a specific task. A knitting chart and a scone recipe are both a kind of algorithm. In the context of AI, algorithms are used to process data and make decisions based on that data. AI systems contain algorithms that help them process specific instructions e.g. how to learn and assign a reward for correct outcomes. An algorithm might help an AI to decide whether a particular piece of content is desirable, or undesirable. Much of the behaviour of modern AI emerges from iterative learning – hence the commonly used term "*machine learning*".

CCIAO (The Christchurch Call Initiative on Algorithmic Outcomes): is an initiative funded and supported by the governments of New Zealand, the United States, and Twitter, Microsoft and OpenMined. It aims to deliver solutions that accelerate research about how social media algorithms affect radicalisation to violence, and the proliferation of TVEC, and help to deliver interventions to address that problem. The CCIAO's first project is to build and test new privacy enhancing technology tools that allow external researchers to ask questions about highly sensitive datasets without being able to directly access the underlying private user information. These tools are widely considered to be a key step in creating effective AI oversight and audit mechanisms.

Civil Society: refers to organisations, individuals, and loose civil coalitions of individuals that advance the interests and will of people independently from the institutional perspectives of business or government. Civil society can refer to technical experts, human rights advocacy groups, non-profits, social enterprises, volunteers, academics and academic institutions and non-governmental organisations, among others.

G7 (the Group of Seven): is an informal intergovernmental political forum consisting of Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, with the participation of the European Union. The G7 has a rotating Chair who hosts meetings to facilitate coordination of economic policy and other trans-national challenges.

Masjidain: the dual form of 'Masjid' meaning a place of worship in Arabic.

Multistakeholder: A multistakeholder approach involves the participation of multiple stakeholders, including civil society, the private sector, and government, in decision-making processes. This approach is often used by internet governance institutions.

Online Service Provider: refers to a company or organisation that provides an electronic service by means of the internet. This includes for instance: social media, gaming, cloud storage, cybersecurity, entertainment, search engines, and online payments providers among many other things.

TVEC (Terrorist and Violent Extremist Content): online content that promotes or incites terrorism or violent extremism. This content can include propaganda, recruitment materials, instructional guides, and other forms of media that encourage or glorify violent acts. Internationally Governments apply different, sometimes conflicting, definitions of terrorism and violent extremism, and most online platforms use a combination of behavioural criteria with information about specific violent groups to identify whether something is TVEC.

Annex 1: Christchurch Call text

Annex 1

CHRISTCHURCH CALL

The Christchurch Call to Action

To Eliminate Terrorist and Violent Extremist Content Online

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

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

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

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

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

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

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

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

Counter the drivers of terrorism and violent 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

To that end, we, Governments and online service providers, commit to work collectively to:

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

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

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

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

Ensure appropriate cooperation with and among law 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.

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

Collaborate, and support partner countries, in the development and implementation of best 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.

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

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

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

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

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

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

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

Cabinet

Minute of Decision

Report of the Cabinet Social Wellbeing Committee: Period Ended 28 July 2023

On 31 July 2023, Cabinet made the following decisions on the work of the Cabinet Social Wellbeing Committee for the period ended 28 July 2023:

SWC-23-MIN-0098	**Update on the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online** Portfolio: Prime Minister	CONFIRMED

[redacted]

Rachel Hayward
Secretary of the Cabinet

Cabinet Social Wellbeing Committee

Minute of Decision

Update on the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online

Portfolio **Prime Minister**

On 26 July 2023, the Cabinet Social Wellbeing Committee:

1 **noted** that the Christchurch Call (the Call), launched in May 2019, forms part of the Government's policy response to the March 15 terror attack and has achieved positive change in the way online service providers, governments, and civil society act to eliminate terrorist and violent extremist content online;

2 **noted** that, as liberal democracies seek ways to manage the risks and opportunities of technologies such as artificial intelligence, New Zealand's co-leadership of the Call (alongside France) has delivered valuable experience in the development of multi-stakeholder solutions and highly relevant work on the impacts of algorithmic processes;

3 **noted** that:

3.1 the Call has an ambitious work programme and faces some challenges to delivery;

3.2 the appointment of a Special Envoy will help to advance this work, and manage any risks, whilst maintaining the profile of the Call as a leading international tech initiative;

4 **invited** the Prime Minister to provide a further progress update to Cabinet 6(a), 9(2)(f)(iv) [redacted]

Rachel Clarke
Committee Secretary

Present:
Rt Hon Chris Hipkins
Hon Carmel Sepuloni
Hon Grant Robertson
Hon Dr Megan Woods
Hon Jan Tinetti
Hon Dr Ayesha Verrall
Hon Priyanca Radhakrishnan
Hon Ginny Andersen
Hon Barbara Edmonds
Hon Willow-Jean Prime
Hon Dr Deborah Russell

Officials present from:
Office of the Prime Minister
Officials Committee for SWC