Australian Government
Department of Home Affairs

Five Country Ministerial Statement on Countering the Illicit Use of Online Spaces

We, the Homeland Security, Public Safety, and Immigration Ministers of Australia, Canada, New Zealand, the United Kingdom, and the United States, stand united in our commitment to protect our citizens from child predators, terrorists, violent extremists and other illicit actors. We are as determined to counter these threats online as we are to counter them in the physical world. We note with disappointment that senior digital industry leaders did not accept our invitation to engage on critical issues regarding the illicit use of online spaces at the 2018 Five Country Ministerial meeting. Nevertheless, we reiterate our determination to work together constructively to ensure our response is commensurate to the gravity of the threat. Our citizens expect online spaces to be safe, and are gravely concerned about illegal and illicit online content, particularly the online sexual exploitation of children. We stand united in affirming that the rule of law can and must prevail online.

We are committed to an open, safe and secure internet; one that provides global connectivity, better access to services, and new ways to conduct business and share news and information. But we recognise that the anonymous, instantaneous and networked nature of the online environment has magnified the threats we face, and has opened up new vectors for harm. We are determined to ensure that the technologies that have been developed to enhance prosperity and freedom are not exploited by those who seek to promote terrorism and violent extremism; prey upon and exploit our children; or spread disinformation and discord to undermine our democratic institutions.

The evolution of digital technology has created new opportunities for widespread transmission of child exploitation material, and for perpetrating the most abhorrent kinds of child sexual exploitation, such as live-streaming of abuse. And it is not only in the recesses of the dark web that such material is accessible. Much is hosted on the most common top-level domains. Moreover, the growing sophistication of mobile technology has enabled offenders to target children, including through apps that can be used to recruit and coerce children to engage in sexual activity. The low financial cost, and the anonymised nature of this criminal enterprise, is contributing to a growth in the sexual exploitation of children. We must escalate government and industry efforts to stop this.

We also affirm the need to build upon efforts to counter the use of the internet by terrorists and violent extremists who continue to exploit online spaces to share materials designed to radicalise and mobilise individuals to violence. These materials are used for recruitment, facilitation, training and financing purposes, often with devastating consequences. Governments and industry have made some progress in tackling this issue. However, the task is far from complete. Terrorists and violent extremists remain able to disseminate propaganda promoting violence, and to use online platforms to radicalise and recruit. And, despite concerted efforts, a great deal of terrorist and violent extremist content remains accessible online to anyone inclined to seek it out. We therefore call upon industry to go further in proactively and innovatively addressing the illicit use of their platforms and applications at pace. In this context we welcome and support the Global Internet Forum to Counter Terrorism (GIFCT). But we urge industry leaders to champion more rapid responses, both under the auspices of the GIFCT and beyond. Digital industry must take responsibility to reduce the availability of online terrorist and violent extremist content across all platforms and applications, and to do so comprehensively. Recognizing the G7 Interior Ministers' statement on terrorism and violent extremism, we echo and amplify their call to action, and we affirm that efforts must extend to all types of illegal and illicit online content.

We are also increasingly seeing the use of online spaces to spread disinformation, sow division, and undermine our democratic institutions. The proliferation of interference activities and disinformation undermines the trust of citizens in online communications and information, delegitimizing the benefits and opportunities that communications and social media platforms create.

We call upon industry to meet public expectations regarding online safety by:

- Developing and implementing capabilities to prevent illegal and illicit content from ever being uploaded, and to execute urgent and immediate takedown where there is a failure to prevent upload.
- Deploying human and automated capabilities to seek out and remove legacy content.
- Acting on previous commitments to invest in automated capabilities and techniques (including photo DNA tools) to detect, remove and prevent re-upload of illegal and illicit content, as well as content that violates a company's terms of service.
- Prioritising the protection of the user by building user safety into the design of all online platforms and services, including new technologies before they are deployed.
- Building upon successful hash sharing efforts to further assist in proactive removal of illicit content.
- Setting ambitious industry standards, and increasing assistance to smaller companies in developing and deploying illicit content counter-measures.
- Building and enhancing capabilities to counter foreign interference and disinformation.
- Preventing live streaming of child sexual abuse on all platforms.

We recognise that governments also have a major role to play in addressing the spread of illicit content online. We commit to build the capacity of non-'five eyes' countries to protect and defend the most vulnerable. We undertake to enhance information flows from government to industry, and work towards overcoming barriers to cross-sectoral collaboration. We agree to ensure our enforcement capabilities, including technical data such as hashes, can be shared with industry to support the development of scalable, Artificial Intelligence-driven solutions. Through the same innovation and cross-sectoral collaboration that has underpinned so many technological advances, the challenge of countering illicit online content is not insurmountable.

To focus our collective efforts, we agree to establish a senior officials group charged with monitoring industry progress on the above actions on a quarterly basis and reporting back to us. We welcome digital industry Chief Executive Officers to future meetings of the Five Country Ministerial to update us on their efforts directly.