The Canadian Government's proposed approach to address harmful content online

GLOBAL PARTNERS DIGITAL

Global Partners Digital submission
September 2021

About Global Partners Digital

Global Partners Digital (GPD) is a social purpose company dedicated to fostering a digital environment underpinned by human rights.

Introduction

We welcome the opportunity to provide feedback on New Zealand's draft principles and objectives for negotiating a new UN convention on cybercrime. Cybercrime can adversely harm the enjoyment of a range of human rights, including the rights to privacy and to freedom of expression. Appropriate legislation, if effectively and fairly enforced, can help enhance human rights, by protecting people's personal data and information (protecting their right to privacy) and ensuring that electronic communication channels remain open and secure (protecting their right to freedom of expression). The development of appropriate frameworks at the national, regional and global levels to combat cybercrime therefore has significant potential in protecting human rights.

At the same time, however, we have seen across the world how measures taken in the name of combating cybercrime can also pose risks to human rights. Overly broad powers for security and law enforcement agencies to investigate potential criminal offences, for example, or overly broad exceptions to criminal offences which protect individual's rights to privacy, can result in unjustified restrictions on the right to privacy. And where cybercrime frameworks prohibit certain forms of online communications, overly broad criminal offences can constitute unjustified restrictions on the right to freedom of expression.

It is therefore essential that any new framework developed to combat cybercrime at the global level be fully informed by, and consistent with, international human rights law and standards.

Our approach

While we remain unconvinced of the need for a new global convention on cybercrime, we recognise that, by virtue of Resolution 74/247[1], the Ad Hoc Committee on Cybercrime has been mandated to elaborate a comprehensive international convention

[1] https://undocs.org/en/A/RES/74/247

on countering the use of information and communications technologies for criminal purposes.

Our approach towards the development of this convention is based on three key principles.

- First, in order to avoid fragmented approaches, any new convention should build on, and be consistent with, existing frameworks and work undertaken in other parts of the UN, including by the Open-ended Intergovernmental Expert Group Meeting on Cybercrime

- Second, the provisions of the convention should be fully consistent with the international human rights framework, including international human rights instruments and their interpretation by authoritative bodies. Of particular relevance to the convention are the rights to privacy and freedom of expression. In line with well-understood principles of international human rights law, any interference will only be justified if there is a clear and precise legal basis, the interference pursues an objectively legitimate aim, and if it is necessary and proportionate. The convention must ensure that its provisions do not directly or indirectly require or justify interferences with these rights that are not permissible under international human rights law.

- Third, given that cybercrime is an issue affecting a wide range of stakeholders, and that expertise in combating cybercrime exists outside of government actors, it is vital that all relevant stakeholders - including civil society - are able to participate meaningfully in the development of the convention.

Feedback on the draft principles and objectives

Based on our approach, we provide the following specific feedback on the draft principles and objectives.

Draft principles

- While the importance of human rights is recognised in the draft objectives, we believe that the effective protection of human rights should also be a principle underpinning New Zealand's approach. We would suggest adding an additional principle: "Advocate for any eventual convention to be informed by, and consistent with, the international human rights framework, including treaties and their interpretation by authoritative UN bodies."

Draft objectives

- The term "harmful content online" in the third objective should be either removed or clearly and narrowly defined. While there are certainly a small number of types of harmful content where there an international consensus on the need to address them (in particular child sexual abuse imagery), for many others there is either no universal consensus on how to define the type of content (e.g. "terrorist material" or "extremist material") or there is no universal consensus that regulatory efforts are needed (e.g. "disinformation"). To ensure

that the new convention, and any content-based criminal offences, does create risks to the right to freedom of expression, it would be helpful if the objectives provided clarity on precisely which types of harmful content should be within scope, and we would urge the government to focus exclusively on those types where there is universal consensus that they need to be addressed through the criminal law and are clearly defined.

- We would suggest greater clarity in the fifth objective as to when it would be appropriate for procedural provisions to apply to offences which do not constitute cybercrimes. Given that many of the measures taken to access electronic evidence are highly intrusive (particularly those that involve surveillance or the collection of communications and other forms of data), a broader discussion would be helpful to take into account broader human rights considerations and to determine what safeguards are needed to ensure that such measures are only used when appropriate and proportionate (for example, only with respect to the most serious offences, only where there is judicial or some other form of authorisation). To reflect this, and to enable that more open discussion, we would recommend rewording the objective as "Recognises that the relevance of digital evidence extends beyond cybercrime and cyber-enabled crime to further offences, and contains provisions relating to appropriate access to electronically stored criminal evidence and the necessary corresponding safeguards.".

Recommendations for implementation

In addition to the feedback on the draft principles and objectives, we also make two recommendations as to how they can be translated into practice:

- The government of New Zealand should advocate as strongly as possible for the process to be as open, inclusive and transparent as possible when the modalities of the sessions are discussed. This means offering opportunities for non-governmental stakeholders, including civil society organisations, to provide input into the decisionmaking process. This should be open not only to organisations with ECOSOC accreditation, but all relevant civil society organisations, through formal meetings with stakeholders, open consultation events, and informal consultations between sessions. If the final modalities are not so inclusive, New Zealand should lead and encourage efforts by like-minded states to provide more informal mechanisms for input and discussion outside of the formal sessions, to help inform national positions.

- At all stages of the convention's development, assessment of draft texts by independent human rights experts should be made and considered by the Ad Hoc Committee. This could either be done formally within the process through a standing committee of experts, by utilising existing expertise within the United Nations Office of the United Nations High Commissioner for Human Rights, or more informally by regularly inviting human rights assessments of drafts from governmental and non-governmental stakeholders.