# GNI Statement on UN Cybercrime Convention

The Global Network Initiative (GNI), the leading global, multistakeholder organization focused on freedom of expression and privacy in the technology sector, is deeply concerned about the latest draft of the United Nations Comprehensive International Convention on Countering the Use of Information and Communications Technologies (ICTs) for Criminal Purposes (hereafter, the 'Convention'). As Member States prepare to finalize the Convention in August, GNI urges them to carefully consider the necessity of this proposed Convention, in light of other existing, proven multilateral frameworks such as the Budapest Convention on Cybercrime. They should also consider the draft's likely impact on privacy, freedom of expression, freedom of assembly and association, gender equality and other internationally recognized human rights. We advise Member States not to agree on a convention that enables criminalization of legitimate online activities protected under international human rights standards, including broad authorizations of state surveillance, contains vague catch-all provisions, and does not meet the highest level of safeguards and human rights protections concerning investigative powers and international cooperation.

The GNI Principles on Freedom of Expression and Privacy and its related Implementation Guidelines set a framework, based on international human rights principles, for responsible tech company conduct, including in the context of engaging with governments around access to data. Over the last 15 years, we have helped a growing range of companies stand up for human rights in the face of overbroad, unjustified, discriminatory, or otherwise inappropriate demands from governments. While we recognize the unique and important role that governments play in addressing cybercrime, we are alarmed by the prospect of a UN treaty that calls upon Member States to affirmatively criminalize and cooperate regarding a broad range of poorly-defined conduct (extending beyond cybercrimes) facilitated by information and communication technologies (ICTs), without sufficiently acknowledging and addressing the risks that accompany the establishment and enforcement of such measures.

For example, the draft Convention in Article 18 is unclear about the liability of online platforms for offenses committed by their users. Unlike subsequent articles, which require intent, Article 18 does not mandate intentional participation in the offenses as defined by the Convention. This discrepancy raises the risk that online intermediaries could be held liable for user-generated content without actual knowledge or awareness of its illegal nature. This could lead to excessively broad content moderation and removal of legitimate, protected speech by platforms, thereby negatively impacting freedom of expression. From our experience monitoring platform regulations around the world, these impacts will disproportionately fall upon marginalized

groups who are already at a higher risk of censorship and surveillance. Questions of intent and *mens rea* are critical to the practical application of criminal law and the treaty's broad language risks empowering overbroad applications, including in the context of children sharing intimate images ("sexting") as set out in Article 16.

A number of UN Member States already implement a broad range of aggressive measures in the name of addressing cybercrime, many of which have been documented to result in human rights abuses – with differentiated impacts – including those targeting vulnerable groups such as ethnic, racial, gender, and religious minorities, journalists, and human rights defenders. The draft Convention in its present form would legitimize such practices, incentivize even more aggressive practices, and make it more difficult for UN bodies, Member States, information and communication technology companies, and civil society watchdogs to push back against them.

As it currently stands, the draft Convention authorizes pervasive cross-border surveillance without requiring the types of safeguards long-understood to be necessary in these contexts under international human rights law and rights respecting practices within data protection frameworks. As such, it risks significantly reshaping the practice of and expectations around the investigation and prosecution of online conduct in ways likely to chill protected activities significantly.

Human rights safeguards should be the baseline for the development of criminal procedural measures, and not the other way around. Despite numerous calls from civil society and government on the articulation of clear and robust protections for human rights, negotiations on the Convention have failed to address and incorporate these elements. For instance, the qualification of the list of safeguards set out in Article 24(2) with the term "as appropriate in view of the nature of the procedure or power concerned," is unnecessary and opens the door for State Parties to deviate from internationally-recognized and appropriate practices.

Robust safeguards, including the principles of non-discrimination, legality, legitimate purpose, necessity and proportionality, requiring independent authorization of law enforcement requests for data, inclusion of the dual-criminality concept in the context of cross-border cooperation, robust transparency around and judicial review of investigatory and prosecutorial conduct, and easily accessible remedial mechanisms, are essential to prevent the misuse of power and protection of individual rights. Effective gender mainstreaming is also essential to ensure the Convention is not used to undermine people's human rights on the basis of gender. Countries committed to human rights and the rule of law must unite to demand stronger data protection and human rights safeguards. Without these they should refuse to agree to the draft Convention.


GLOBAL
NETWORK
INITIATIVE