

COMMITTEE: Human Rights 1

QUESTION OF: Balancing counter-terrorism measures with civil liberties, with focus on the so-called “chat control”

SUBMITTED BY: Canada, Finland, Azerbaijan, Greece

CO-SUBMITTED BY: Madagascar, Panama, Greece, Guyana, UK, Brazil, Bangladesh, Venezuela

SIGNATORIES: Estonia, Panama, Guyana, Denmark, Finland, Nigeria, Madagascar, Afghanistan, France

The General Assembly,

Recalling the Universal Declaration of Human Rights, particularly Article 12, which protects individuals from arbitrary interference with privacy, correspondence, and communications,

Reaffirming the International Covenant on Civil and Political Rights (ICCPR), especially Articles 17 and 19, guaranteeing the right to privacy and freedom of expression, recognizing the legitimate responsibility of States to prevent and combat terrorism and serious crimes, including online child exploitation and extremist activities,

Alarmed by the growing use of mass digital surveillance technologies, commonly referred to as “Chat Control,” which may involve the automated scanning of private electronic communications,

Acknowledging the adoption of counter-terrorism legislation such as Canada’s Anti-Terrorism Act Bill-C51, and the International Security Act, designed to address modern security threats including terrorism and cyber enabled crimes,

1. Encourages the integration of clear legal safeguards within counter-terrorism laws, ensuring that security measures are:

- a. Necessary and proportionate,
- b. Based on clearly defined security objectives,
- c. Subject to judicial authorization and review;

2. Calls upon Member States, drawing on the Canadian model, to strengthen independent oversight and data protection frameworks by:

- a. Promoting structured collaboration between parliamentary oversight committees, independent national security review agencies, privacy commissioners, and civil liberties organizations;
- b. Reinforcing and modernizing national privacy legislation, including privacy acts, to guarantee that residents have the right to access information held about them by government authorities;
- c. Establishing clear, accessible, and effective procedures for the correction or deletion of inaccurate, outdated, or unlawfully collected personal data;
- d. Mandating the regular publication of transparency reports detailing the scope, legal basis, and oversight of state data collection and surveillance practices.

3. Affirms that Member States must establish strong oversight and accountability mechanisms to prevent abuse of surveillance powers and to ensure full compliance with international human rights and data protection laws:

- a. Making sure if international human rights are not respected or not met, with proper consequences like: criminalization, discharged from service, or suspension,
- b. The Consequences would be according to the severity, and frequency of these breaches of human rights

4. Encourages the implementation of educational campaigns all over the world, that would propagate governments inclusion on surveillance of citizens data, and what the governments are doing, why are they doing it, and where does it do it:

- a. The educational campaigns would be combined with youth forums, in charge of educating citizens on governments actions,
- b. The educational campaigns would be funded by NGOs such as Teach For All (TFA) and funds from the UNHCR;

5. Calls upon Member States to develop balanced legal frameworks addressing online safety and chat control that:

- a. Uphold end-to-end encryption as a fundamental tool for protecting personal data, journalist integrity and confidential communication,
- b. Ensure that any measures aimed at monitoring or regulating digital communication are lawful, necessary, proportionate, and subject to clear judicial oversight,
- c. Avoid the creation of systemic vulnerabilities, including backdoors or weakened encryption standards, that could be exploited by malicious actors,
- d. Draw inspiration from national legislative experiences, including those of the United Kingdom, while adapting policies to domestic legal systems and international human rights obligations;

6. Stresses the critical role of cybersecurity in ensuring the safe use of encrypted communication technologies and effective online governance, and calls upon Member States to strengthen cybersecurity frameworks through:

- a. The development and regular updating of comprehensive national cybersecurity strategies that protect digital infrastructure, encrypted communication platforms, and personal data from cyberattacks, data breaches, and unauthorized access,

- b. The establishment of clear standards and best practises for public and private sector actor regarding cyber risk management, incident response, and system resilience,
- c. Increased investment in cybersecurity research, innovation, and workforce training to address emerging threats and reduce vulnerabilities within digital systems,
- d. Enhanced international cooperation through information-sharing mechanisms, joint capacity-building initiatives, and multilateral dialogue to address cross-border cyber threats and promote collective digital security,
- e. The promotion of public-private partnership to improve cybersecurity preparedness while ensuring that security measures do not undermine encryption or violate fundamental human rights;

7. Calls for the regulation on the role of private platforms through;

- a. Mandating transparency reports on all state data request;
- b. Explicitly prohibiting platforms from acting as law enforcement substitutes;
- c. Independent and multi-layered oversight with national review agencies with binding power;
- d. Lawful cooperation for clear defined penalties for misuse or overuse

10. Clarifies that any data used for counter-terrorism and chat control purposes shall be obtained exclusively through lawful, targeted, and transparent mechanisms, including:

- a) Civilian law enforcement agencies acting under domestic criminal law and judicial authorization;
- b) Civilian intelligence agencies, where permitted by national law, subject to parliamentary and judicial oversight;
- c) Military or defense intelligence entities, only when threats meet the legal threshold of national security or armed conflict, and solely through cooperation with civilian authorities;

d) Private digital platforms, responding only to formal, lawful data requests and not through proactive or mass surveillance;

12. Calls upon all member states to support and fund the “United Nations Organization of Chat Oversight” (UNOCO):

- a. To open their intelligence regarding terrorism up to the UNOCO;
- b. For member states that are part of this committee particularly to open their law enforcement to allow for a clearer and effective method by which the UN Security Council's Counter-Terrorism Committee (CTC) and the Human Rights Committee may make decisions to oversee an individual or organization's private or public social media and chats;
- c. The organization will be manned by the UN Security Council's Counter-Terrorism Committee (CTC) and funded by member states of the United Nations and corporate donations
 - i. Member states will annually contribute .0005% percent of GDP
 - ii. Payments will be due on March 1 of each calendar year

13. Reaffirms the current cooperation amid member states in the European Union to share control over social media and social media terrorism:

- a. All member states should contribute financially, as needed;
- b. Sharing control: All member states have the same rights to initiate or to suspend an online investigation. All member states whose delegates belong to the Security Council and the Human Rights Committee also have access to the same information and task force in regards to occurring online investigations;

14. Recommends the creation of the “United Nations Organization of Chat Oversight” (UNOCO) which will:

- a. Will require the labor of intelligence organizations, law enforcement, and government representatives;
- b. The organization is to have a task force dedicated primarily to the cause, and they will be in charge of setting up the investigation and going through with it;
- c. The aims of this commission is the following:

- i. This commission hopes to achieve the goal of balancing the need for chat control within the sphere of Terrorism, while still respecting the right of privacy granted to all the citizens of the world,
 - ii. The Committee will meet semi-annually to discuss any and all reported cases of suspicion of terrorism, all possible information attained for said cases, and forward their findings to the Security Council who will then come to a decision over whether or not to investigate the individual (70% majority vote), which then gets sent to the Human Rights Committee for approval.
- d. UNOCO will use no Ai, and will be filtered by professionals having passed training in International laws;

15. All the members deal with collected data on the country's national level, only if submitted by the state does the UNOCO have the right to deal with the problem on an international level.

- a. Calls for the adoption of targeted surveillance measures focused only on individuals or networks with credible evidence of criminal or terrorist activity:
 - i. National evidence regarding "Criminal activity" and "terrorist activity" will be defined by each member state for their own nation and they provide evidence that they perceive as in need of international cooperation or attention to promote national sovereignty;
 - ii. Nation states may vote in a assembly over what will constitute as terrorism specifically
 - 1. 70% majority vote will pass the understanding of what terrorism is
 - iii. Targets acts of cyber-enabled violence, coercion, or disruption that are premeditated and political in objective, and that directly threaten life, physical safety, essential services, or critical infrastructure,
- b. Each violation has to be submitted to the (UNOCO) by national level intelligence organizations which would apply following consequences based on the severity.

16. Suggests that all digital communication services operating within the jurisdiction would be allowed to implement automated systems capable of detecting illegal and harmful content in real time:

- a. Providers must promptly report detected illegal content to designated national authorities and the International Digital Protection Agency (IDPA) without delay;
- b. Chat control mechanisms shall be updated regularly to address emerging threats and criminal techniques;
- c. Each sovereign country is able to decide whether or not to use “Chat control”
- d. Reminds sovereign countries that legally they have to give information on any individual or organization suspected of relating or being terrorists,
- e. Having the UNOCO as a filtering system that cleans data, and prioritizes the jurisdiction of certain information,