CFMUN

Security Council

Topic A: "Establishing International Frameworks for Digital Surveillance: Balancing Security and Privacy in the New Global Era"

Welcoming letter

Dear delegates,

Welcome to the Security Council committee. It is our pleasure to have you participating in this committee as we address the topic **“Establishing International Frameworks for Digital Surveillance: Balancing Security and Privacy in the New Global Era”** during the *CFMUN XII* edition. This issue lies at the core of today’s humanitarian and security challenges, as advancements in digital surveillance raise new questions about how secure is our privacy. You will have to think critically, communicate clearly, and work alongside the other delegates to accomplish the best possible solution for this issue.

We encourage you to approach this committee with professionalism, respect, and an open mind. Whether you are an

experienced delegate or it is your first time in the Security Council, your contributions will shape the progress and quality of the debate. Remember that diplomacy, collaboration, and creativity are key to achieving meaningful outcomes. We are excited to see your dedication throughout the sessions and are confident that your participation will make this *CFMUN XII* edition a memorable and enriching experience.

We wish all delegates the best of luck, and welcome once again to *CFMUN XII*.

Sincerely,
Fabiola Castro and Inés Hernández

CFMUN

Table of contents

I. Committee Background

The United Nations Security Council (UNSC) is the UN body with primary responsibility for maintaining international peace and security. It is the only UN organ with the power to adopt coercive measures and decisions that are legally binding on all Member States.

It focuses on:

Peaceful settlement of disputes: The main focus is on conflict prevention, urging disputing parties to resolve their differences through peaceful means such as negotiation, mediation, arbitration, or judicial settlement.

Peacekeeping: When conflicts arise, the Council establishes and deploys peacekeeping operations to stabilize situations, monitor ceasefires, and protect civilians.

II. Introduction to the Topic

In today's rapidly evolving digital landscape, surveillance technologies have become essential tools for national and international security. However, their expansion raises pressing concerns about privacy, transparency, and the protection of fundamental rights. The lack of a unified international framework has led to uneven practices and potential risks of misuse across borders. In this committee, delegates will examine how the global community can establish effective international standards for digital surveillance while ensuring a fair balance between security and privacy in the modern era.

CFMUN

III. Evolution of the Topic

Digital surveillance has evolved rapidly alongside technological development. In the early 2000s, governments focused mainly on monitoring communications to address rising security threats, especially after 9/11. As smartphones, social media, and data-storage technologies expanded during the 2010s, surveillance became more widespread and sophisticated, raising global concerns about privacy—especially after the Snowden revelations in 2013.

In recent years, tools like artificial intelligence, facial recognition, and biometrics have further increased the reach and accuracy of digital surveillance. While these technologies strengthen national security and help combat cybercrime, they also heighten risks of misuse and human rights violations. This evolution has highlighted the growing need for clear international standards to balance security with the protection of individual privacy.

IV. Relevant Events

A) Panorama

Digital surveillance has expanded rapidly over the past two decades, driven by technological innovation and increasing threats to global security. After 9/11, many countries increased their monitoring of communications to prevent terrorism and cybercrime. The rise of smartphones, social media, and cloud data in the 2010s made surveillance more sophisticated and widespread, raising significant privacy concerns, especially after the Snowden revelations in 2013.

More recently, tools such as artificial intelligence, biometrics, and facial recognition have strengthened government's ability to track individuals in real time. While these technologies contribute to national security and help prevent cyberattacks, they also increase the risks of misuse, a lack of transparency, and human rights violations.

Since each country regulates digital surveillance differently, the world faces a fragmented landscape without clear international standards. This situation hinders cooperation and highlights the need for a global framework that balances security with the protection of individual privacy.

B) Points of View

United States of America

The United States considers digital surveillance essential for national security, counterterrorism, and cybersecurity. While it supports advanced surveillance technologies, internal debates continue regarding privacy, transparency, and oversight. The United States seeks to maintain robust security capabilities while addressing civil liberties concerns.

People's Republic of China

China prioritizes state-controlled surveillance to ensure social stability and internal security. The government extensively monitors online and offline activity to prevent crime and manage

society. This approach is often criticized internationally for its limited transparency and potential human rights violations.

Germany (on behalf of the European Union)

Germany promotes a balance between security and privacy, emphasizing legal safeguards, independent oversight, and compliance with human rights standards.

Surveillance is permitted but strictly regulated to ensure accountability and transparency.

United Nations

The UN encourages international cooperation and the creation of frameworks that balance security with privacy. It highlights the importance of transparency, accountability, and the protection of human rights in surveillance practices.

V. UN and External Actions

UN Actions

The United Nations has addressed digital surveillance primarily through human-rights frameworks and international dialogue. Key efforts include:

- Human Rights Council Resolutions: Affirm the right to privacy online and offline, urging states to ensure surveillance respects human rights.
- Special Rapporteur on the Right to Privacy: Publishes reports on the impact of state and corporate surveillance, calling for transparency and accountability.
- International Telecommunication Union (ITU): Promotes cybersecurity standards and responsible data management.
- Workshops and Forums: The UN hosts discussions among states, civil society, and private actors to develop principles for ethical surveillance and cross-border cooperation.

UN actions focus on promoting human rights,

transparency, and dialogue, but they are largely nonbinding.

External Actions

Outside the UN, several states and organizations have implemented important measures:

- European Union (GDPR): Sets strict standards for data collection, privacy, and cross-border transfers, indirectly regulating surveillance.
- United States: Uses legislation like the PATRIOT Act and the CLOUD Act to enhance security while relying on oversight mechanisms to protect privacy.
- China: Maintains extensive state-controlled surveillance for internal security, raising international human rights concerns.
- Israel: Develops and exports advanced surveillance technologies, used worldwide for cybersecurity and counterterrorism.
- Multilateral initiatives: Organizations like the OECD and the Council of Europe promote ethical data use, privacy protection, and cross-border cooperation.

VI. Conclusion

Digital surveillance is a defining challenge of the modern global era. While technological advancements offer states powerful tools to increase security, combat terrorism, and address cyber threats, they also raise serious concerns about privacy, transparency, and human rights. The current absence of a unified international framework has led to inconsistent practices, potential abuses, and tensions between national security priorities and individual freedoms.

Moving forward, it is essential for the international community to work collaboratively to establish clear standards that balance security with the protection of privacy. Such frameworks should promote transparency, accountability, and ethical use of technology, ensuring that advancements in digital surveillance serve global safety without compromising fundamental rights.

VII. Committee Focus

The Security Council must determine how to balance national security needs with the protection of civil liberties. Key areas include:

- How much should the international community regulate digital surveillance without interfering with the nations decisions?
- What basic rules should an international framework include to protect both security and people's privacy?
- How can the UN help prevent the misuse of surveillance tools—like spyware or facial recognition—against journalists, political opponents, or important figures around the world?
- Should digital espionage between countries be considered a threat to international peace and security, and how should it be addressed?
- What role should the UN and technology

companies have in controlling and monitoring the use and sale of advanced spyware such as Pegasus?

CFMUN

VIII. Participation List

- Argentine Republic
- Canada
- The Commonwealth of Australia
- Federative Republic of Brazil
- Federal Republic of Germany
- French Republic
- Italian Republic
- Japan
- Kingdom of Denmark
- Kingdom of Norway
- Kingdom of Spain
- Kingdom of the Netherlands
- New Zealand
- People’s Republic of China
- Republic of Chile
- Republic of Colombia
- Republic of Iceland
- Republic of India
- Republic of Kenya
- Republic of South Africa
- Republic of South Korea
- Republic of Türkiye

- Republic of the Philippines
- Russian Federation
- State of Israel
- United Arab Emirates
- United Kingdom of Great Britain and Northern Ireland
- United Mexican States
- United States of America

IX. References

Amnesty International. (2023, December 12). EU's decision not to ban mass public surveillance in the AI Act sets a devastating global precedent. https://www.amnesty.org/en/latest/news/2023/12/eu-decision-not-to-ban-mass-surveillance

Centre for International Governance Innovation. (2025). International legal regulation of autonomous technologies. https://www.cigionline.org/articles/international-legal-regulation-autonomous-technologies/

Council of Europe. (2024). Guidelines on the responsible use of AI in systems of public surveillance. https://www.coe.int/en/web/artificial-intelligence

Davison, N. (2016). A legal perspective: Autonomous weapon systems under international humanitarian law.International Committee of the Red Cross. https://www.icrc.org/en/download/file/65762/autonomous_weapon_systems_under_international_humanitarian_law.pdf

Derechos Digitales. (2022). Informe vigilancia masiva OEA / RELE. https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf

International Committee of the Red Cross. (2025). Autonomous weapon systems and International Humanitarian Law: Selected issues. https://www.icrc.org/en/article/autonomous-weapon-systems-and-international-humanitarian-law-selected-issues

International Telecommunications Union. (2023). AI governance and cross-border data protection.
https://www.itu.int

Kellogg, K. (2023). The geopolitics of digital authoritarianism. Journal of Democracy.
https://www.journalofdemocracy.org

NATO Cooperative Cyber Defence Centre of Excellence. (2024). Legal and ethical considerations of autonomous defense systems.
https://ccdcoe.org

UN Human Rights Council. (2023). Report on the right to privacy in the digital age.
https://www.ohchr.org

United Nations Office for Disarmament Affairs. (2024). Lethal autonomous weapons systems: Updated UN positions and state submissions.
https://unoda.org