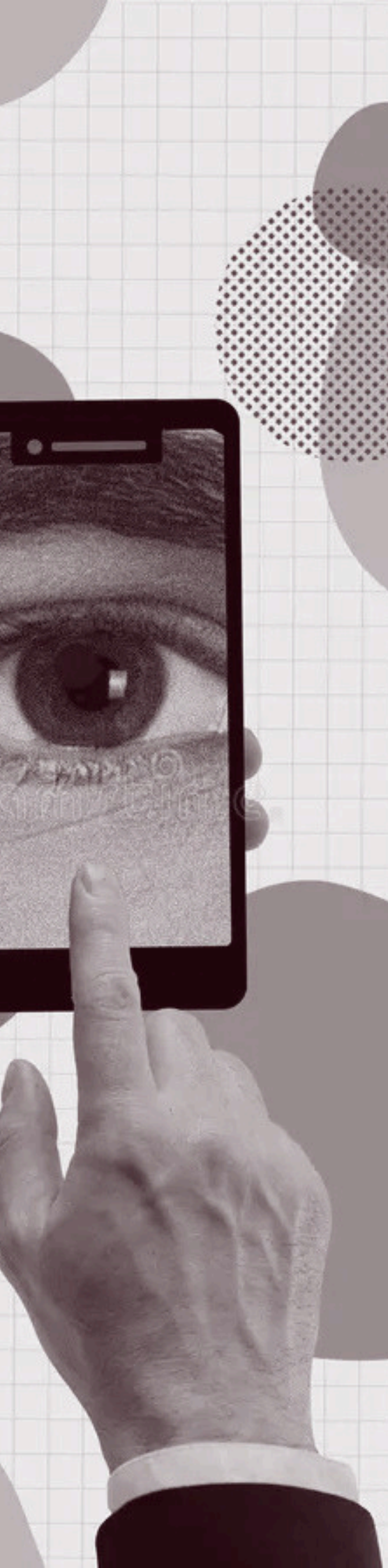




Defending the right to privacy in the digital age

STUDY GUIDE





INDEX

<u>Letter from your chairs</u>	03
<u>Committee introduction</u>	05
<u>Introduction to the topic</u>	07
<u>Key terms</u>	08
<u>Historical Background</u>	10
<u>Current situation</u>	12
<u>Solutions</u>	13
<u>Bloc positions</u>	15
<u>Questions a resolution paper must answer</u>	16
<u>References</u>	18

LETTER FROM YOUR CHAIR

Dear Delegates;

Welcome to this year's SPMUN Human Rights Council! My name is Marypaz Murillo, and I am excited to serve as your co-chair alongside Guisia. I am in tenth grade and I've taken part in three Model United Nations before, participating in UNHRC on all three occasions.

Beyond MUN, you might recognize me from the school play, the girls' volleyball team, or academic activities. If you're ever hesitant to jump into school activities, my advice is simple: take the risk! The experiences and people you meet are always worth it.

If this is your first time taking part in SPMUN (which may be the case for a lot of you), I'll give you some tips: Make sure to research your country's position well, understand their point of view. Make sure you comprehend the issue correctly and identify your allies among all delegates. Also, do not be afraid to speak! I know it may feel intimidating, but at the end of the day, we were all starting once and you shouldn't feel judged for making your point of view (or rather, your delegation's) known.

Guisia and I will do everything to encourage you guys to participate and make you feel welcome and comfortable. We also want our committee to be a space for respectful coexistence; please always remember to be respectful towards your fellow delegates and towards the cultures and countries being represented. Both Guisia and I are available to you if you need help with anything or have any concerns, so don't hesitate to reach out if that were the case.

Best wishes from your chair,
Marypaz Murillo.

LETTER FROM YOUR CHAIR

Dear Delegates,

Welcome to the Human Rights Council at SPMUN! My name is Guisia, and I am thrilled to be serving as your co-chair this year alongside Marypaz. I've been involved in Model UN since seventh grade, so I completely understand how overwhelming that first committee session can feel.

Outside of MUN, you can usually find me participating in Semana Cultural. Stepping up to speak in committee isn't all that different from walking onto our school gym and performing; it takes a bit of courage, but the rush of taking that risk is worth every second. If you ever feel hesitant to raise your placard, just remember that every experienced delegate started out in your exact shoes.

Marypaz and I are dedicated to making this committee a supportive, engaging environment where everyone feels confident sharing their perspectives. To get the most out of this experience, I encourage you to dive deep into your delegate research, stay open to forming strategic alliances, and keep your debate grounded in mutual respect for all cultures and viewpoints represented in the room.

We can't wait to see the creative solutions you bring to the floor and watch you grow into persuasive diplomats throughout the conference. If you ever need a hand with committee procedure, public speaking, or resolution writing, our door is always open!

Best wishes,

Guisia Gomez.

COMMITTEE INTRODUCTION

The United Nations Human Rights Council is the intergovernmental body within the United Nations system made up of 47 States.

They are responsible for strengthening the promotion and protection of human rights around the globe and for addressing situations of human rights violations. It has the ability to discuss all thematic human rights issues and situations that require its attention throughout the year. Established in 2006, it provides a multilateral forum to address human rights violations and country situations. It responds to human rights emergencies and makes recommendations on how to better implement human rights on the ground. The Council benefits from substantive, technical, and secretariat support from the Office of the High Commissioner for Human Rights (OHCHR).

The main functions of the Council include:

- Serving as an international forum for dialogue on human rights issues with UN officials and mandated experts, states, civil society, and other participants.
- Adopting resolutions or decisions during regular sessions that express the will of the international community on given human rights issues or situations. Adopting a resolution sends a strong political signal which can prompt governments to take action to remedy those situations.

COMMITTEE INTRODUCTION

- Holding crisis meetings (a.k.a special sessions) to respond to urgent human rights situations.
- Reviewing the human rights records of all United Nations Member States via the Universal Periodic Review.
- Appointing the Special Procedures; independent human rights experts who serve as the eyes and ears of the Council by monitoring situations in specific countries or by looking at specific themes.
- Authorizing commissions of inquiry and fact-finding missions, which produce hard-hitting evidence on war crimes and crimes against humanity.

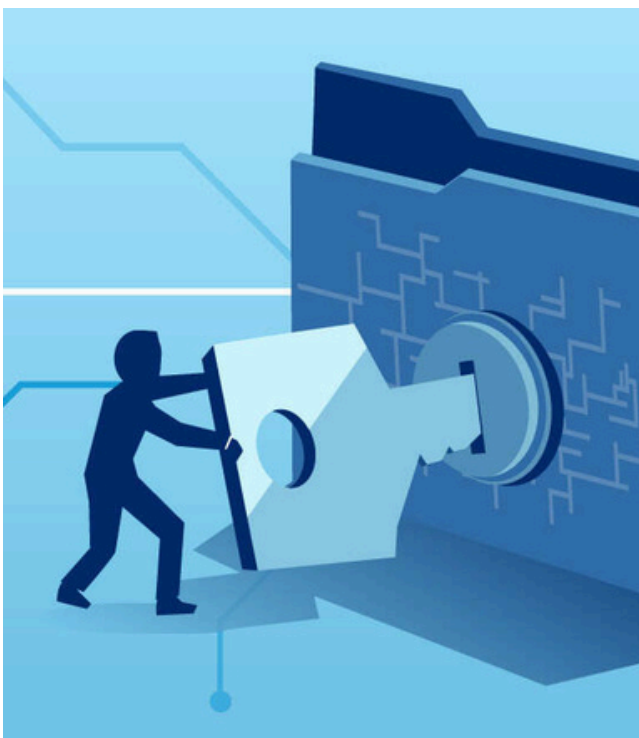
The UNHRC is the governing body in charge of reviewing the defense of the right to privacy. Privacy enables the enjoyment of other rights: the free development and expression of an individual's personality, identity and beliefs, and their ability to participate in political, economic, social and cultural life. The right to privacy surged in the Universal Declaration of Human Rights (1948) – Article 12; as it expressed that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."

In 2015, the Human Rights Council created the first official assignment, scope of authority, and set of responsibilities given to an appointed independent expert on privacy in resolution 28/16. The mandate was renewed for a period of three years in March 2024 .

INTRODUCTION TO THE TOPIC

With the development of technology in recent years, the concern of privacy violations has shifted from just “wanting to be left alone” to wanting to protect personal data from the recollection and processing of it by data-intensive technologies. Digital technologies do not exist in a vacuum; technology cannot be understood, evaluated, or regulated as an isolated tool. Instead, every software, algorithm, or digital system is shaped by—and directly impacts—the social, legal, political, and

economic environments in which it operates. They can be a powerful tool for advancing human progress and contribute greatly to the promotion and protection of human rights. However, data-intensive technologies, such as artificial intelligence applications contribute to creating a digital environment in which both States and business enterprises are increasingly able to track, analyze, predict and even manipulate people’s behavior to an unprecedented degree. These technological developments carry very significant risks for human dignity, autonomy and privacy and the exercise of human rights in general, if applied without effective safeguards.





KEY TERMS

OHCHR: Office of the United Nations High Commissioner for Human Rights.

Data intensive technologies: Systems where the biggest challenge is managing massive amounts of fast-moving, complicated data, rather than just needing faster computers.

Metadata: Data about data, providing structured information that describes, explains, locates, or gives context to other information.

Data Minimization: The principle that organizations should only collect, process, and retain the absolute minimum amount of personal data necessary to fulfill a specific, stated purpose.

Purpose Limitation: The requirement that personal data collected for one explicit reason cannot be used for secondary, unrelated purposes without obtaining new consent.

Informed Consent: A user's explicit, unambiguous, and voluntary agreement to allow an entity to process their personal data, given only after clear details about usage are provided.

Data Brokerage: The commercial practice of aggregating, analyzing, and selling personal details compiled from public records, app usage, and online tracking to third parties.



KEY TERMS

End-to-End Encryption: A communications security system where only the communicating users can read the messages—preventing third parties, Internet Service Providers, and even the service provider itself from accessing the unencrypted data.

Mass Surveillance: The indiscriminate monitoring, tracking, or collecting of digital activity and communications belonging to large populations by state entities or private corporations.

Digital Footprint: the trail of data left behind by an individual's online activities, consisting of active footprints (posts, emails) and passive footprints (IP addresses, browsing histories, location logs).

HISTORICAL BACKGROUND

The concept of privacy was born from philosophy and has had long historical roots in both anthropological and sociological discourses.

Despite having a long history of evolution, the right to privacy has just been evident in the late 19th century. Privacy was first recognized by Article 12 of the Universal Declaration of Human Rights, 1948 (UDHR), following the widespread state abuses and mass surveillance during World War II. Consequently, international bodies elevated privacy from a domestic legal concept to an inviolable international human right; although it started with the view of protecting one's bodily integrity and home from unwarranted intrusion, the concept of privacy turned soon toward control over personal information. In 1966, the International Covenant on Civil and Political Rights (ICCPR), Article 17 transformed the UDHR principles into a legally binding international treaty, obligating signatory nations to enact protective domestic legislation.



HISTORICAL BACKGROUND

The issue of digital privacy violations began taking shape in the late 20th century with early computer databases, but it reached a crisis point after 2001 when post-9/11 national security laws accelerated bulk data collection. This shift was driven by the rapid rise of internet communications, the expansion of mass surveillance programs, and the 2013 Snowden revelations, which exposed how government intelligence agencies and private tech giants gather metadata and private records without individual consent. While mass surveillance networks span globally, populations in democratic nations with high digital connectivity, states with expansive state-monitoring infrastructure, and politically vulnerable or dissident groups face the most direct impact on their civil liberties. Ultimately, this issue persists because technology, artificial intelligence, and corporate data harvesting evolve far faster than national laws and international oversight can regulate them, leaving personal data exposed to misuse.



CURRENT SITUATION

Digital privacy has become a growing international issue because governments and private companies have access to more personal information than ever before. Surveillance technologies such as spyware can be used to access phones, messages, locations, and other private information. While governments argue that these technologies are necessary for national security and preventing crime, they can also be misused against journalists, activists, and political opponents. Countries have different laws and opinions about how much surveillance should be allowed, which makes it difficult to create international rules. Because technology continues to develop, the international community needs to find a balance between protecting national security and defending the fundamental right to privacy.

SOLUTIONS

1. Create stronger international regulations for spyware

The international community should establish clear rules for the development, sale, export, and use of commercial spyware. Governments should only use these technologies for legitimate security purposes and under strict legal requirements. Companies should also be prevented from selling spyware to governments that may use it to violate human rights.

2. Establish independent oversight systems

Countries should create independent organizations to supervise government surveillance programs. These organizations should investigate possible abuses and verify that surveillance is legal, necessary, and proportionate. The use of highly invasive spyware should also require authorization from an independent judicial body.

3. Protect journalists, activists, and human rights defenders

Governments should create special protections for journalists, activists, political opponents, and human rights defenders. These individuals should not be targeted simply because they criticize a government, investigate corruption, or defend human rights. Stronger protections would help defend freedom of expression and prevent the misuse of surveillance technologies.

4. Create mechanisms for victims to receive justice

People who have been unlawfully surveilled should have access to investigations, legal assistance, notification when possible, and other forms of remedy. Governments and private companies responsible for violating privacy rights should be held accountable for their actions.

SOLUTIONS

5. Improve international cooperation

Countries should cooperate through the United Nations and other international organizations to share information about surveillance threats and investigate possible abuses. International cooperation could also help create common standards for digital privacy and make it more difficult for governments or companies to avoid responsibility.

6. Balance national security with the right to privacy

Surveillance should not be completely prohibited because governments may need it to investigate serious crimes, terrorism, or national security threats. However, surveillance must have a legitimate purpose and should only be used when necessary. Governments should always choose the least invasive method available.

BLOC POSITIONS

China:

China places a great deal of emphasis on national security, state sovereignty, and maintaining government control over digital information. The country may support the use of surveillance technologies to address issues like terrorism, espionage, and cyber threats. However, China is likely to be cautious about international regulations that might interfere with its domestic surveillance practices.

United States

The United States views surveillance as a crucial tool for ensuring national security, preventing terrorism, and aiding in criminal investigations. With its substantial intelligence operations and influential technology firms, the U.S. plays a significant role in discussions about digital privacy. While it may advocate for stronger regulations, it also defends the legitimate use of surveillance.

Israel:

Israel is a key player in the surveillance conversation, especially due to its role in developing and producing commercial spyware. The country may support using surveillance technologies for national security and law enforcement. Meanwhile, international discussions often focus on holding spyware companies accountable and the importance of regulating the export of these technologies.

Germany:

Germany typically champions enhanced human rights protections and demands greater accountability for surveillance technologies. It advocates for independent oversight, strict legal requirements, and safeguards for journalists and activists. Germany is also likely to support international collaboration to prevent the misuse of spyware.

QUESTIONS A RESOLUTION PAPER MUST ANSWER

As delegates debate over digital rights, you will tackle critical dilemmas where technological innovation intersects with fundamental human freedoms. You can use these questions as a guide of the contents of the resolution papers that will be voted upon.

- What international cooperation is required to bridge global digital divides (internet access, local language inclusion, digital literacy) while establishing safeguards for individual control over personal data and protecting marginalized populations from data exploitation?
- What can be done to ensure the criteria of data minimization, purpose limitation, and meaningful consumer consent are always met by data-driven corporations without significantly damaging their performance?
- Given the accuracy flaws and discriminatory impacts of automated facial recognition and surveillance tools, to what extent should governments establish strict regulations on government surveillance in public spaces, and how should this balance against public security?
- What can be done to punish and hold technology companies accountable for human rights violations?
- How can mandatory human rights impact assessments be operationalized across the data lifecycle, and where do matters of child safety intersect with these corporate obligations?

QUESTIONS A RESOLUTION PAPER MUST ANSWER

- How can developers and operators solve the "black box" problem to ensure transparency, external auditing, and the systematic elimination of bias in automated decision-making systems, while navigating tensions surrounding government encryption and law enforcement access?

REFERENCES

A Brief Introduction to the Right to Privacy – An International Legal Perspective - GlobaLex. (n.d.). [Www.Nyulawglobal.Org](https://www.nyulawglobal.org/globalex/Right_To_Privacy_International_Perspective.html). Retrieved September 16, 2026, from https://www.nyulawglobal.org/globalex/Right_To_Privacy_International_Perspective.html

Brian Nougères, Ana. Report of the Special Rapporteur on the right to privacy. A/HRC/58/58. 16 January 2025.

Brian Nougères, Ana. Report of the Special Rapporteur on the right to privacy: elements for a model law on neurotechnologies and neurodata processing. A/80/283. 2025.

Council of Europe. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108+"). CETS No. 223. 10 October 2018.

Court of Justice of the European Union. Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems("Schrems II"). Case C-311/18. 16 July 2020.

OHCHR. (n.d.). *OHCHR / OHCHR and privacy in the digital age.*

Ohchr. Retrieved September 16, 2026, from <https://www.ohchr.org/en/privacy-in-the-digital-age>

OHCHR / Right to privacy in the digital age. (2025). Ohchr.

<https://www.ohchr.org/en/calls-for-input/2025/right-privacy-digital-age>

OHCHR / Special Rapporteur on the right to privacy. (n.d.). Ohchr. Retrieved September 16, 2026, from

<https://www.ohchr.org/en/special-procedures/sr-privacy>

REFERENCES

OHCHR. The right to privacy in the digital age. A/HRC/27/37. 30 June 2014.

OHCHR. The right to privacy in the digital age. A/HRC/51/17. 4 August 2022. <https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age>

OHCHR. The right to privacy in the digital age. A/HRC/60/45. 29 August 2025. <https://www.ohchr.org/en/documents/thematic-reports/ahrc6045-right-privacy-digital-age-report-office-united-nations-high>

Supreme Court of India. Justice K.S. Puttaswamy (Retd.) v. Union of India. (2017) 10 SCC 1. 24 August 2017

UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris, 23 November 2021.

UN General Assembly. Guidelines for the Regulation of Computerized Personal Data Files. A/RES/45/95. 14 December 1990.

UN General Assembly. United Nations Convention against Cybercrime. A/RES/79/243. 24 December 2024. <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>

UN General Assembly. International Covenant on Civil and Political Rights, Art. 17. A/RES/2200(XII)A. 16 December 1966.

UN General Assembly. Pact for the Future, Annex I: Global Digital Compact. A/RES/79/1. 22 September 2024. <https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact>

REFERENCES

UN General Assembly. The right to privacy in the digital age.

A/RES/68/167. 18 December 2013.

<https://undocs.org/en/A/RES/68/167>

UN General Assembly. The right to privacy in the digital age.

A/RES/75/176. 16 December 2020.

<https://digitallibrary.un.org/record/3896430>

UN General Assembly. The right to privacy in the digital age.

A/RES/77/211. 15 December 2022.

UN General Assembly. United Nations Convention against

Cybercrime. A/RES/79/243. 24 December 2024.

[https://www.unodc.org/unodc/en/cybercrime/convention/home.htm](https://www.unodc.org/unodc/en/cybercrime/convention/home.html)

l

UN General Assembly. Universal Declaration of Human Rights, Art.

12. A/RES/217(III)A. 10 December 1948.

UN Human Rights Committee. General Comment No. 16: Article 17

(Right to UN Human Rights Council. The right to privacy in the digital

age. A/HRC/RES/54/21. 12 October 2023.

UN Human Rights Council. Mandate of the Special Rapporteur on

the right to privacy. A/HRC/RES/55/3. March 2024.

<https://www.ohchr.org/en/special-procedures/sr-privacy>

United Nations Human Rights Council. (2024). HRC Home. Ohchr.

<https://www.ohchr.org/en/hrbodies/hrc/home>

United Nations Human Rights Council. (2025). Welcome to the

Human Rights Council. Ohchr; United Nations Human Rights

Council. <https://www.ohchr.org/en/hr-bodies/hrc/about-council>

REFERENCES

United Nations Office of the High Commissioner for Human Rights. (2025). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights* (Document No. A/HRC/60/45). General Assembly, Human Rights Council.