



UNHRC



DELIBERATING ON
STATE SURVEILLANCE VS RIGHT TO PRIVACY
IN DIGITAL AGE

INDEX

I. Letter from the executive board.....	3
II. Suggested Patterns for Researching.....	4
III. Committee Overview.....	5
IV. Introduction.....	6
V. What is state surveillance	7
VI. Understanding Right to Privacy	8
VII. Protection of right to privacy	9
VIII. Causes of disruption in privacy.....	10
IX. Vulnerable groups.....	11
X. International Legal & Institutional Frameworks.....	14
XI. UNHRC’S Role.....	20
XII. Focus Questions.....	22

I. Letter from the Executive Board

Greetings Delegates!

It gives us immense pleasure to welcome you all to this simulation of the **United Nations Human Rights Council (UNHRC) at 'DPS Karnal MUN 2026'**. We look forward to an enriching and rewarding experience.

The agenda for the session is: ***“Deliberating on state surveillance VS Right to privacy in digital age”***

This study guide is by no means the end of the research, we would very much appreciate it if the members are able to find new realms in the agenda and bring it forth to the committee. Such research combined with good argumentation and a solid representation of facts is what makes an excellent performance.

In the session, the executive board will encourage you to speak as much as possible, as fluency, diction, or oratory skills have very little importance as opposed to the content you deliver. So prime emphasis on research is recommended.

The Executive Board looks forward to an efficient & progressive committee as the issue is very sensitive. We, therefore, expect you all to play your roles with responsibility. Hopefully we, as members of the Executive Board, will also have a chance to gain insight from this committee.

All the best!

Regards,

Virat Dahiya
Chairperson

Harshita Singhal
Vice Chairperson

II. Suggested Pattern for Researching

To start researching on the agenda of the committee, participating members should do the following:

1. Start researching your respective countries and its geopolitics. As no definite document may be found which contains the stand of a country, the delegates must do the tedious yet rewarding work of going through past news clippings/ magazine articles/ government websites/ social media handles/ YouTube videos to understand the country's stance on the said agenda.
2. After gaining knowledge about the portfolios, the delegates must start their research on the agenda at hand. This must be done by researching further upon the agenda using the footnotes and links given in the guide and from other sources such as academic papers, institutional or governmental reports, national reports, news articles, blogs etc.
3. Characterize the agenda into sub-topics and prepare speeches and statements on them. The delegates should also prepare a list of possible solutions and actions the UNHRC can suggest/adopt on the issue.
4. Assemble proof/evidence for any important piece of information/ allegation you are going to use in committee and keep your research updated using various news sources, specifically government studies or data released by the same.
5. To have an edge in the committee in terms of debate, delegates must also research about the other countries and try to find their contradictory statements or controversial stands on various issues to raise allegations/ substantial questions in the committee.
6. Lastly, we would expect all the delegates to put in serious efforts in research and preparation for the simulation and work hard to make it a fruitful learning experience for all. Feel free to contact the undersigned if you have any queries or doubts.

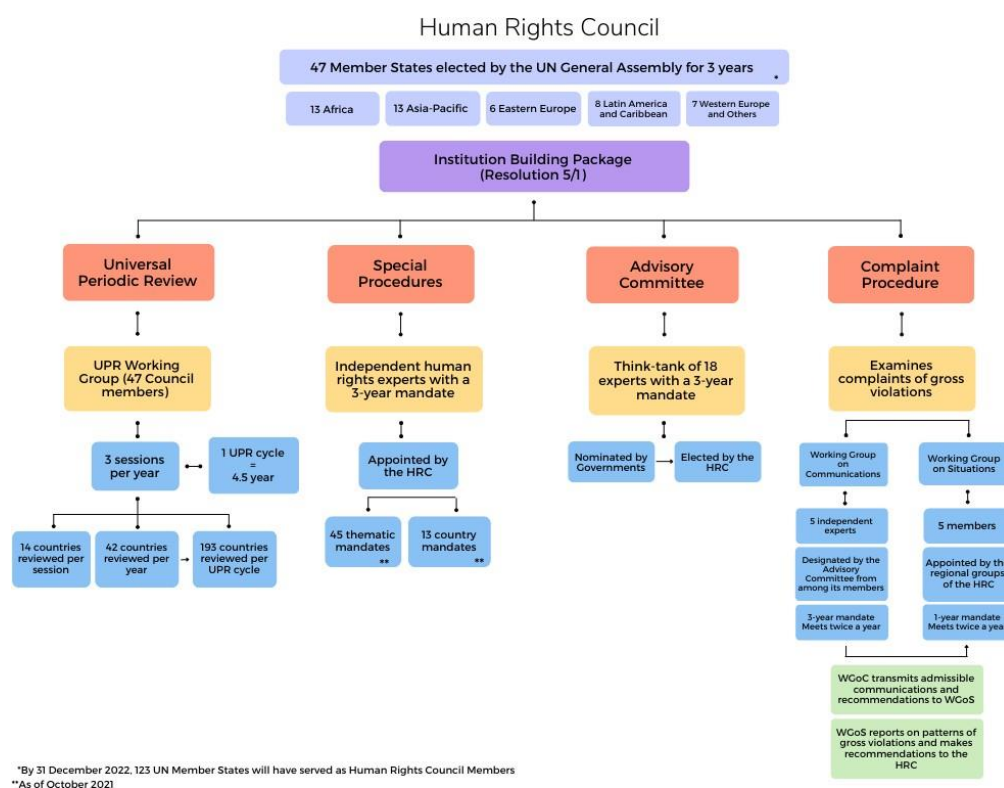
III. Committee Overview

About UNHRC

The United Nations Human Rights Council (UNHRC) is a United Nations body whose mission is to promote and protect human rights around the world.

The Council investigates allegations of breaches of human rights in United Nations member states and addresses thematic human rights issues like freedom of association and assembly, freedom of expression, freedom of belief and religion, women's rights, LGBT rights, and the rights of racial and ethnic minorities.

In 2006 the The United Nations Human Rights Council replaced the United Nations Commission on Human Rights. Its main purpose is addressing situations of human rights violations and making recommendations on them. Its mandate was established by General Assembly resolution 60/251 from 15 March 2006.



IV. Introduction

The digital revolution has fundamentally transformed the way societies communicate, govern, and protect national security. With the widespread use of artificial intelligence, facial recognition, biometric identification, internet monitoring, and large-scale data collection, governments today possess unprecedented capabilities to monitor digital activities. While these technologies have become valuable tools in combating terrorism, cybercrime, organized crime, and other security threats, they have simultaneously sparked an important global debate regarding the protection of the fundamental right to privacy.

The United Nations Human Rights Council (UNHRC) recognizes privacy as an essential human right and a cornerstone of individual dignity, freedom, and democratic governance. Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibit arbitrary or unlawful interference with an individual's privacy, family, home, or correspondence. The Council has consistently affirmed that the same rights people enjoy offline must also be protected in the digital environment.

As digital technologies continue to evolve, the challenge before the international community is not whether surveillance should exist, but how it can be conducted responsibly. States have a legitimate obligation to safeguard national security and public order; however, surveillance measures must remain lawful, necessary, proportionate, transparent, and subject to effective oversight. Excessive or indiscriminate surveillance can undermine public trust, restrict freedom of expression, and threaten other fundamental human rights.

Against this backdrop, the agenda "**Deliberating on State Surveillance vs. Right to Privacy in the Digital Age**" invites Member States to explore a balanced approach that addresses modern security challenges while ensuring that technological advancement remains firmly rooted in the principles of international human rights law.

V. What is state surveillance

Surveillance is the monitoring, collection, and analysis of information about individuals or groups by governments or other entities through physical or digital means for purposes such as security, law enforcement, or intelligence gathering. In the UNHRC, the key debate is ensuring that such surveillance is lawful, necessary, proportionate, and respects the fundamental right to privacy.

Types of Surveillance

Physical Surveillance: Monitoring individuals through CCTV cameras, drones, or direct observation.

Communications Surveillance: Intercepting phone calls, emails, text messages, or internet traffic.

Digital Surveillance: Tracking online behaviour through social media monitoring, metadata collection, cookies, AI algorithms, and internet service providers.

Biometric Surveillance: Using fingerprints, facial recognition, iris scans, or voice recognition to identify and track individuals.

Mass Surveillance: Large-scale, indiscriminate collection of data from entire populations rather than specific suspects.

Why do governments conduct surveillance?

Governments may use surveillance to:

Prevent terrorism and violent extremism, Combat cybercrime and organized crime, protect national security, investigate criminal activities, Maintain public order during emergencies, etc

Why is it controversial?

Surveillance becomes controversial when it is **excessive, unlawful, or lacks accountability**. Unchecked surveillance may:

- Violate the **right to privacy**.
- Restrict freedom of expression and association.
- Enable political repression or censorship.
- Target journalists, activists, or minority groups.
- Lead to misuse or unauthorized sharing of personal data.

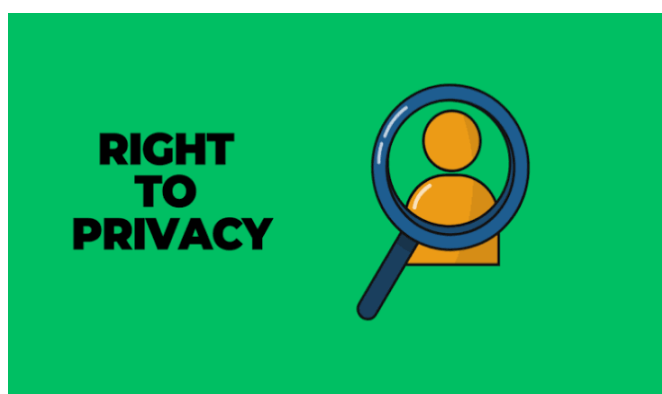
VI. Understanding Right to Privacy

The right to privacy is a fundamental human right that protects individuals from arbitrary or unlawful interference with their personal lives, communications, homes, and personal information. In the digital age, this protection extends beyond physical spaces to encompass online activities, electronic communications, biometric data, and digital identities. As governments increasingly rely on digital technologies for governance and security, safeguarding privacy has become a central concern of the international human rights framework.

The right to privacy is enshrined in **Article 12 of the Universal Declaration of Human Rights (UDHR)** and **Article 17 of the International Covenant on Civil and Political Rights (ICCPR)**, both of which prohibit arbitrary or unlawful interference with an individual's privacy, family, home, or correspondence. Recognizing the rapid growth of digital technologies, the United Nations Human Rights Council (UNHRC) has affirmed that **the same rights people enjoy offline must also be protected online**, reinforcing privacy as a cornerstone of human dignity, autonomy, and democratic participation.

Within the scope of this agenda, privacy also includes an individual's right to control how personal data is collected, stored, processed, and shared. Technologies such as facial recognition, artificial intelligence, geolocation tracking, and mass data collection have significantly expanded governments' surveillance capabilities, making effective legal safeguards increasingly important.

The UNHRC recognizes that the right to privacy is not absolute. States may impose lawful restrictions to protect national security, public order, or prevent crime. However, under international human rights law, any interference must satisfy the principles of **legality, necessity, proportionality, and accountability**. The challenge before Member States is therefore to ensure that security measures protect citizens without eroding the fundamental rights and freedoms that privacy safeguards.



VII. Protection of right to privacy while surveillance of state

Protecting the right to privacy in the digital age requires a combination of strong laws, transparent governance, technological safeguards, and public accountability. The first step is establishing comprehensive legal frameworks that clearly define when and how surveillance may be conducted. Such laws should specify the authorities empowered to carry out surveillance, the circumstances under which it is permitted, and the duration and scope of data collection. Equally important is ensuring that surveillance requests are subject to prior judicial authorization or independent oversight to prevent arbitrary or politically motivated monitoring.

Governments should adopt the principles of **data minimization** and **purpose limitation**, collecting only the information necessary for a specific and legitimate objective while prohibiting its use for unrelated purposes. Personal data should be stored securely, protected through encryption and cybersecurity measures, and permanently deleted once it is no longer required. Transparency reports, independent audits, and parliamentary review further strengthen public confidence by allowing citizens to understand how surveillance powers are exercised.

Individuals also play a vital role in protecting their privacy. The use of strong passwords, multi-factor authentication, encrypted communication platforms, regular software updates, and greater awareness of digital risks can significantly reduce vulnerabilities. At the international level, cooperation among states is essential to regulate cross-border data transfers, establish common standards for emerging technologies such as artificial intelligence and facial recognition, and ensure that digital innovation remains consistent with international human rights law. By combining effective oversight with responsible technological practices, states can protect both national security and the fundamental right to privacy in an increasingly interconnected world.

VIII. Causes of disruption in privacy

The rapid expansion of digital technologies has significantly increased the risk of privacy violations across the globe. One of the primary causes is the widespread use of **mass surveillance**, where governments collect large volumes of communications, metadata, internet activity, and location information without individualized suspicion. While often justified on grounds of national security or crime prevention, indiscriminate surveillance can result in excessive monitoring of ordinary citizens and undermine fundamental human rights.

Another major factor is the advancement of **artificial intelligence (AI), facial recognition, and biometric technologies**. These systems enable authorities to identify, track, and profile individuals in real time, often without their knowledge or consent. In the absence of clear legal safeguards, such technologies may lead to discriminatory practices, wrongful identification, and misuse of personal data.

The growing collection and commercialization of personal information by private technology companies also contributes to privacy concerns. Vast amounts of user data including browsing history, location, financial transactions, and social media activity are routinely collected, creating opportunities for unauthorized access, data breaches, or sharing with third parties. Governments may also request or compel access to such data, further expanding surveillance capabilities.

Cross-border data transfers, cyberattacks, and the use of sophisticated spyware have further intensified these challenges. Commercial surveillance software has been used in several instances to monitor journalists, political opponents, and human rights defenders, raising concerns about unlawful interference and the suppression of civil liberties. Weak data protection laws, limited judicial oversight, inadequate cybersecurity, and a lack of transparency collectively increase the risk of privacy violations. Addressing these issues requires stronger legal frameworks, independent oversight, and international cooperation to ensure that technological advancements do not come at the expense of fundamental human rights.

IX. Vulnerable groups

Although digital surveillance has the potential to affect every individual, its impact is far from equal. Certain groups face significantly greater risks because of their profession, identity, political opinions, or social status. These communities are often subjected to heightened monitoring, data collection, profiling, or targeted surveillance, making them more vulnerable to violations of their fundamental rights. The United Nations Human Rights Council (UNHRC) has repeatedly emphasized that surveillance technologies should never be used to suppress dissent, discriminate against communities, or undermine democratic participation.

Journalists and Media Professionals

Journalists rely on confidential communication to investigate corruption, expose human rights abuses, and hold governments accountable. Unlawful surveillance compromises source confidentiality, discourages whistle-blowers from sharing information, and weakens press freedom. The emergence of sophisticated spyware capable of accessing messages, microphones, cameras, and encrypted communications has significantly increased these risks.

Women journalists face an even greater burden. According to UNESCO, **73% of women journalists have experienced online violence, while one in four reported that online attacks escalated into offline violence or threats**, creating a chilling effect that forces many to self-censor or withdraw from public discourse.

Human Rights Defenders and Civil Society Organizations

Human rights defenders, lawyers, trade union leaders, environmental activists, and non-governmental organizations frequently challenge abuses of power and advocate for vulnerable communities. Consequently, they are often subjected to surveillance intended to monitor their activities, identify networks, or discourage advocacy.

The Office of the United Nations High Commissioner for Human Rights (OHCHR) has warned that commercial surveillance technologies have increasingly been deployed against activists and civil society organizations, undermining freedom of association and peaceful assembly. The fear of constant monitoring discourages participation in protests, advocacy campaigns, and public debate, weakening democratic institutions.

Political Opposition and Whistleblowers

Opposition politicians, election campaign staff, whistleblowers, and individuals exposing governmental misconduct are particularly vulnerable to targeted surveillance. Monitoring private communications can reveal political strategies, confidential information, and personal relationships, giving authorities an unfair advantage and potentially influencing democratic processes.

International investigations submitted to the OHCHR have alleged that **over 300 journalists, lawyers, judges, diplomats, political figures, and activists in India were identified as potential targets of Pegasus spyware**, highlighting the misuse of advanced surveillance technologies beyond legitimate law enforcement purposes.

Women and Girls

Women experience surveillance differently because privacy violations often intersect with gender-based violence. Stolen personal information, hacked devices, location tracking, intimate image abuse, and spyware have been used for stalking, domestic abuse, blackmail, and harassment.

According to UNESCO, **58% of young women and girls globally have experienced online harassment**, while AI-generated deep fakes and image manipulation have further intensified digital abuse. These forms of surveillance disproportionately silence women participating in journalism, politics, activism, and public life by creating fear of retaliation and reputational harm.



Ethnic, Religious, and Marginalized Communities

Artificial intelligence and facial recognition technologies are increasingly used in policing and border management. However, studies have shown that algorithmic bias and unequal deployment of surveillance technologies may disproportionately affect marginalized communities.

Research submitted to the OHCHR concerning India found that facial recognition technology and predictive policing could disproportionately target marginalized populations, particularly Muslim communities in Delhi, because of existing policing patterns and structural biases. Without adequate safeguards, surveillance technologies risk reinforcing discrimination rather than promoting public safety.

Refugees, Migrants, and Stateless Persons

Refugees and migrants often possess limited legal protections and may be required to submit extensive biometric information, including fingerprints, iris scans, facial images, and personal records, to obtain humanitarian assistance or cross international borders. While biometric registration improves aid delivery and identity verification, inadequate safeguards may expose these populations to unauthorized data sharing, profiling, or surveillance by state and non-state actors.

Because refugees frequently flee persecution by governments, the unauthorized disclosure of their personal information may place them or their families at further risk, making robust privacy protections essential.



Children and Young People

Children represent one of the fastest-growing digital populations, yet they frequently lack the awareness or legal capacity to understand how their personal data is collected and processed. Educational technologies, mobile applications,

gaming platforms, and social media services routinely gather information on children's behaviour, location, preferences, and online interactions. The widespread integration of artificial intelligence into digital platforms raises concerns regarding long-term profiling, behavioural prediction, and targeted advertising. The UN human rights framework stresses that children's best interests must remain a primary consideration whenever their personal data is collected or processed.

Why Protecting Vulnerable Groups Matters

For the UNHRC, protecting vulnerable groups extends beyond safeguarding individual privacy; it is essential for preserving **freedom of expression, freedom of association, political participation, access to justice, and democratic governance**. When surveillance is conducted without transparency, judicial oversight, or accountability, its effects are rarely distributed equally. Instead, it disproportionately burden those already at greater risk of discrimination or persecution. Ensuring that surveillance remains **lawful, necessary, proportionate, and non-discriminatory** is therefore indispensable to protecting both national security and universal human rights in the digital age.

X. International Legal & Institutional Frameworks

The rapid expansion of digital technologies has outpaced the development of international legal frameworks governing surveillance and privacy. While international law recognizes that states may conduct surveillance for legitimate purposes such as national security, counter-terrorism, and crime prevention, it also establishes strict safeguards to ensure that such measures do not result in arbitrary or unlawful interference with fundamental human rights. The international framework governing this agenda is therefore built upon human rights treaties, United Nations resolutions, institutional oversight mechanisms, and emerging principles on digital governance.

1. Universal Declaration of Human Rights (UDHR), 1948

The foundation of the international privacy regime lies in **Article 12 of the Universal Declaration of Human Rights (1948)**, which states:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Although the UDHR is not legally binding, it forms the cornerstone of modern international human rights law and has influenced numerous constitutions, treaties, and domestic privacy legislation across the world.

2. International Covenant on Civil and Political Rights (ICCPR), 1966

The **International Covenant on Civil and Political Rights (ICCPR)** is the primary legally binding international treaty governing the right to privacy.

Article 17 provides:

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."

Unlike the UDHR, the ICCPR imposes legally binding obligations on its **174 State Parties** to respect and protect the right to privacy.

The **UN Human Rights Committee**, through **General Comment No. 16 (1988)**, clarified that:

- surveillance must never be arbitrary,
- states must establish effective legal safeguards,
- personal data must not be collected indiscriminately,
- individuals should have access to legal remedies against unlawful surveillance.

These principles continue to guide judicial interpretation worldwide.

3. UN Human Rights Council Resolution 34/7 (2017)

Recognizing the increasing use of digital surveillance technologies, the **UN Human Rights Council adopted Resolution 34/7**, titled:

"The Right to Privacy in the Digital Age."

The Resolution:

- reaffirms that human rights protected offline also apply online;
- expresses concern regarding unlawful and arbitrary surveillance;
- urges Member States to review domestic surveillance laws;
- encourages independent oversight mechanisms;
- calls upon states to ensure surveillance complies with international human rights obligations.

This remains one of the Council's most significant policy documents addressing digital privacy.

4. UN General Assembly Resolution 68/167 (2013)

Following global concerns over mass electronic surveillance, the **UN General Assembly unanimously adopted Resolution 68/167: "The Right to Privacy in the Digital Age."**

The Resolution:

- recognizes privacy as a prerequisite for freedom of expression;
- condemns arbitrary mass surveillance;
- requests states to review surveillance practices;
- called upon the UN High Commissioner for Human Rights to prepare the first comprehensive report on digital privacy.

This marked the first major UN response to large-scale digital surveillance practices.

5. Office of the United Nations High Commissioner for Human Rights (OHCHR)

The **OHCHR** serves as the principal UN institution responsible for monitoring implementation of international human rights standards.

Its landmark **2014 Report on "The Right to Privacy in the Digital Age"** concluded that:

- mass surveillance may violate international human rights law;
- metadata deserves protection comparable to communication content;
- indiscriminate surveillance is rarely compatible with the principles of necessity and proportionality;
- judicial authorization and independent oversight are essential safeguards.

Since then, the OHCHR has produced multiple thematic reports addressing:

- AI and human rights,
- biometric surveillance,
- facial recognition,
- commercial spyware,
- cross-border data transfers.



6. UN Special Rapporteur on the Right to Privacy

Established by the Human Rights Council in **2015**, the **Special Rapporteur on the Right to Privacy** is an independent expert mandated to:

- investigate privacy violations,
- conduct country visits,
- communicate directly with governments,
- recommend legislative reforms,
- report annually to both the Human Rights Council and the General Assembly.

The mandate has become increasingly significant as surveillance technologies continue to evolve.

7. General Data Protection Regulation (GDPR) — European Union (2018)

Although a regional regulation, the **General Data Protection Regulation (GDPR)** has become the global benchmark for privacy legislation.

Key principles include:

- lawfulness and fairness,
- purpose limitation,
- data minimization,
- accuracy,
- storage limitation,

- accountability.

The GDPR grants individuals:

- the right to access personal data,
- the right to correction,
- the right to erasure ("Right to be Forgotten"),
- the right to data portability,
- protection against automated decision-making.

As of **2025**, numerous countries—including Brazil, Japan, South Korea, Kenya, South Africa, and several ASEAN members—have enacted or updated privacy laws inspired by GDPR principles.

8. Convention 108+ (Council of Europe)

The **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)** is the world's only legally binding international treaty dedicated exclusively to data protection.

The modernized **Convention 108+** expands protections concerning:

- biometric information,
- genetic data,
- automated decision-making,
- cross-border data transfers,
- AI governance.

Importantly, the Convention is open to **non-European states**, reflecting its growing global significance.



9. International Court of Justice (ICJ)

Although the **International Court of Justice** has not directly adjudicated a case solely concerning digital surveillance, its jurisprudence reinforces broader principles of state responsibility, respect for sovereignty, and compliance with international treaty obligations. These principles are increasingly relevant where cross-border surveillance activities affect the rights of individuals in other jurisdictions.

10. Global Digital Landscape: Key Statistics

The urgency of strengthening international legal frameworks is reflected in the rapid expansion of digital technologies:

- According to the **International Telecommunication Union (ITU)**, **5.8 billion people (approximately 71% of the global population)** were using the Internet by the end of **2024**.
- **GSMA** estimates that more than **5.8 billion people** now own mobile devices, making smartphones the primary source of personal data worldwide.
- The **global surveillance technology market** was valued at **approximately USD 170 billion in 2024** and is projected to exceed **USD 300 billion by the early 2030s**, driven by investments in artificial intelligence, facial recognition, and smart-city infrastructure.
- More than **140 countries** have enacted comprehensive data protection or privacy legislation, demonstrating growing international recognition of digital privacy as a legal right. However, significant differences remain in enforcement, oversight, and safeguards against state surveillance.

Significance for the UNHRC

The international legal framework demonstrates that **privacy is not an absolute right**, nor is state surveillance inherently unlawful. Instead, international human rights law requires that surveillance measures satisfy the principles of **legality, legitimate aim, necessity, proportionality, transparency, accountability, and effective judicial oversight**. The challenge before the UNHRC is to strengthen these safeguards in an era where artificial intelligence, biometric surveillance, and cross-border data flows continue to evolve faster than existing legal and institutional mechanisms.

XI. UNHRC's Role in This Agenda and Key Challenges

The **United Nations Human Rights Council (UNHRC)** is the principal intergovernmental body responsible for promoting and protecting human rights globally. While it does not possess legislative or enforcement powers over Member States, it serves as the primary platform for developing international human rights standards, facilitating dialogue, and encouraging states to uphold their obligations under international law. In the context of "**Deliberating on State Surveillance vs. Right to Privacy in the Digital Age**," the Council seeks to strike a balance between states' legitimate security interests and the protection of fundamental human rights.

A. Role of the UNHRC

1. Developing International Human Rights Standards

The UNHRC formulates international norms through resolutions, thematic discussions, and expert consultations. It has adopted landmark resolutions such as **34/7 (2017)**, **42/15 (2019)**, and **48/4 (2021)** on *The Right to Privacy in the Digital Age*, reaffirming that **the same rights individuals enjoy offline must also be protected online**. These resolutions encourage Member States to review surveillance laws, strengthen privacy protections, and ensure compliance with international human rights standards.

2. Monitoring State Compliance

Although the Council cannot impose legally binding sanctions, it monitors the human rights practices of all **193 UN Member States** through the **Universal Periodic Review (UPR)**. During this peer-review mechanism, countries are evaluated on their surveillance legislation, data protection policies, judicial safeguards, and compliance with international human rights obligations. States are encouraged to implement recommendations made by fellow Member States and independent experts.

3. Supporting Independent Investigations

The UNHRC works closely with the **Office of the United Nations High Commissioner for Human Rights (OHCHR)** and the **Special Rapporteur on the Right to Privacy**. These independent mechanisms conduct country visits, investigate allegations of unlawful surveillance, publish thematic reports, and recommend legislative and institutional reforms to ensure surveillance practices remain lawful, necessary, proportionate, and accountable.

4. Promoting International Cooperation

Digital surveillance frequently extends beyond national borders through cloud computing, multinational technology companies, and cross-border data transfers. The Council therefore encourages international cooperation to develop common standards on cybersecurity, artificial intelligence, biometric surveillance, and data protection while respecting the sovereignty of Member States.

5. Protecting Vulnerable Communities

The Council consistently highlights the disproportionate impact of unlawful surveillance on journalists, human rights defenders, political opponents, lawyers, minorities, women, refugees, and civil society organizations. Through its resolutions and investigations, the UNHRC advocates for safeguards that prevent surveillance technologies from being misused to suppress dissent, restrict civic space, or facilitate discrimination.

B. Challenges Before the UNHRC

1. Balancing National Security and Human Rights

Perhaps the greatest challenge is reconciling two equally important objectives: protecting national security and safeguarding individual rights. While governments require surveillance to combat terrorism, cybercrime, espionage, and organized crime, excessive or indiscriminate surveillance can undermine the rights to privacy, freedom of expression, and freedom of association. Establishing a universally accepted balance remains one of the Council's most complex responsibilities.

2. Rapid Technological Advancements

Emerging technologies such as **artificial intelligence, facial recognition, predictive policing, biometric identification, quantum computing, and commercial spyware** are evolving much faster than international legal frameworks. This technological gap makes it difficult for the Council to develop timely and comprehensive human rights standards.

3. Jurisdictional and Cross-Border Challenges

Digital communications and personal data routinely cross-national borders, while surveillance operations may involve multiple jurisdictions. Differences in national privacy laws, cybersecurity regulations, and intelligence-sharing agreements complicate international accountability and cooperation.

4. Limited Enforcement Powers

Unlike international courts, the UNHRC cannot compel states to amend their domestic laws or impose penalties for violations. Its effectiveness largely depends on political consensus, diplomatic engagement, peer pressure, and the willingness of Member States to implement its recommendations voluntarily.

5. Misuse of Surveillance Technologies

Reports by the **OHCHR** and other UN mechanisms have highlighted the misuse of surveillance technologies against journalists, opposition leaders, activists, lawyers, and human rights defenders. Preventing these technologies from becoming instruments of political repression while allowing their legitimate use for law enforcement remains an ongoing challenge.

6. Regulating the Private Sector

Private technology companies increasingly develop and sell surveillance software, artificial intelligence systems, biometric databases, and spyware to governments worldwide. Ensuring corporate transparency, accountability, ethical development, and respect for human rights has become a growing priority for the UNHRC.

Conclusion

As digital technologies continue to reshape governance and security, the UNHRC plays a central role in promoting a **human rights-based approach to surveillance**. While it cannot prohibit surveillance altogether, the Council seeks to ensure that all surveillance measures comply with the universally accepted principles of **legality, legitimate purpose, necessity, proportionality, transparency, accountability, and independent oversight**. The Committee's ultimate objective is to foster international cooperation that enables states to protect both **national security** and the **fundamental rights and freedoms** that form the foundation of democratic societies.

XII. Focus Questions

1. How can the UNHRC strengthen international standards to ensure that state surveillance complies with the principles of legality, necessity, proportionality, and accountability?
2. What role should the UNHRC play in promoting global norms for the ethical use of artificial intelligence, facial recognition, biometric technologies, and other emerging surveillance tools?
3. How can the UNHRC encourage Member States to balance national security interests with the protection of the right to privacy without infringing upon state sovereignty?

4. Should the UNHRC recommend the development of a comprehensive international framework or convention governing digital privacy and state surveillance?
5. How can the Universal Periodic Review (UPR) mechanism be better utilized to assess national surveillance practices and encourage reforms?
6. What measures can the UNHRC recommend to ensure greater transparency, judicial oversight, and public accountability in state surveillance programmes?
7. How can the UNHRC strengthen the protection of journalists, human rights defenders, whistleblowers, lawyers, political dissidents, and civil society organizations from unlawful or politically motivated surveillance?
8. What role should private technology companies play in ensuring that surveillance technologies are developed, exported, and used in accordance with international human rights standards?
9. How should the international community regulate the commercial sale and cross-border transfer of intrusive surveillance technologies, including spyware and AI-powered monitoring systems?
10. What international safeguards should be established to regulate the collection, storage, sharing, retention, and deletion of personal data obtained through state surveillance?
11. How can the UNHRC promote international cooperation to combat terrorism, cybercrime, and transnational organized crime while safeguarding fundamental human rights?
12. What mechanisms can be established to ensure effective remedies and accountability for individuals whose right to privacy has been violated through unlawful surveillance?
13. How can developing countries strengthen digital governance and privacy protections despite limited technological and financial resources?
14. In what ways can the UNHRC improve cooperation with the Office of the High Commissioner for Human Rights (OHCHR), the International Telecommunication Union (ITU), UNESCO, and other UN bodies to promote a human rights-based approach to digital governance?
15. As surveillance technologies continue to evolve, what long-term strategies should the UNHRC adopt to ensure that innovation supports both global security and the universal protection of human rights?