Topic A: The Right to Privacy and Freedom of Expression in the Digital Age

Introduction

The expansion of digital technologies has intensified concerns surrounding the right to privacy, as protected under Article 12 of the Universal Declaration of Human Rights (UDHR). Government surveillance practices, including mass data collection and monitoring of online communications, risk arbitrary interference with privacy and may deter individuals from exercising other fundamental rights.[1] As personal identities increasingly exist through online data and digital avatars, violations of digital privacy directly undermine human dignity and autonomy. Such surveillance raises concerns not only for privacy but also for freedom of expression and access to information, as individuals may self-censor or avoid digital platforms due to fear of monitoring.

Freedom of expression, guaranteed by Article 19 of the UDHR, is similarly challenged by internet censorship and content restrictions. The United Nations has affirmed that freedom of expression applies equally online and offline, and that unjustified limitations weaken democratic participation and access to information.[2] Such restrictions conflict with Sustainable Development Goal 16, which emphasizes transparent institutions and the protection of fundamental freedoms as foundations for peaceful and inclusive societies.[3]

The emerging concept of the "right to be forgotten" reflects growing efforts to protect individuals from the lasting harms of permanent digital records. While not formally codified in UN treaties, it aligns with UN principles on privacy and data protection.[4] Balancing this right with the public's right to information requires a human-rights-based approach to digital governance, as emphasized in the UN Roadmap for Digital Cooperation.[5] This balance is essential to ensuring that human rights remain protected in evolving digital environments. However, if misapplied, the right to be forgotten could be exploited to justify censorship, obscure historical records, or limit access to information, potentially undermining transparency and accountability in both public and private sectors.

Current Situation

Government surveillance practices have significantly affected the realization of the right to privacy across diverse national contexts. In the United States and the United Kingdom, expanded digital surveillance frameworks introduced for counterterrorism purposes have raised concerns

[1] United Nations General Assembly. (2022). *The right to privacy in the digital age* (A/RES/77/211).
[2] UNESCO. (2018). *UN Human Rights Council resolution on online freedom of expression and privacy*.
[3] United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*.
[4] Office of the United Nations High Commissioner for Human Rights. (2020). *The right to privacy in the digital age*.
[5] United Nations Secretary-General. (2020). *Roadmap for Digital Cooperation*.

regarding mass data collection and insufficient oversight. United Nations reports have cautioned that indiscriminate surveillance, even when conducted in the name of national security, may constitute arbitrary interference with privacy under international human rights law.[6] In response to public and international scrutiny, both states have implemented legal reforms aimed at increasing transparency and limiting bulk data collection. For example, introducing judicial oversight mechanisms and restricting the duration of data retention to ensure accountability and protect individual privacy. These developments illustrate the challenge faced by democratic societies in reconciling security objectives with obligations under Article 12 of the Universal Declaration of Human Rights (UDHR).

Restrictions on freedom of expression through internet censorship have had profound impacts in other regions. In countries such as China and Iran, extensive filtering of online content, platform restrictions, and surveillance of digital communications have constrained access to information and limited political participation. The United Nations Human Rights Council has repeatedly expressed concern that such practices violate Article 19 of the UDHR, which guarantees the right to seek, receive, and impart information regardless of frontiers.[7] UN mechanisms have identified Internet shutdowns and content blocking as particularly harmful, as they restrict civic space and disproportionately affect journalists, human rights defenders, and marginalized groups.[8] Despite these challenges, UN resolutions and reports continue to promote international standards that affirm the need to protect freedom of expression equally online and offline.

In contrast, some states and regional bodies have adopted stronger regulatory frameworks to protect digital rights. The European Union's General Data Protection Regulation (GDPR) is frequently cited in UN discussions as a best-practice model for safeguarding privacy, enhancing data protection, and addressing concerns related to the "right to be forgotten."[9] By granting individuals greater control over personal data and establishing accountability mechanisms for both governments and private actors, such frameworks support human dignity in digital spaces. These efforts align with Sustainable Development Goal 16, which emphasizes accountable institutions and the protection of fundamental freedoms.[10]

[6] United Nations General Assembly. (2022). *The right to privacy in the digital age* (A/RES/77/211).
[7] United Nations Human Rights Council. (2012). *The promotion, protection and enjoyment of human rights on the Internet* (A/HRC/20/L.13). United Nations.
[8] Office of the United Nations High Commissioner for Human Rights. (2022). *Internet shutdowns: Trends, causes, and human rights impacts*. United Nations.
[9] Office of the United Nations High Commissioner for Human Rights. (2020). *The right to privacy in the digital age*. United Nations.
[10] United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*. United Nations.

Conclusion

The intersection of privacy and freedom of expression in the digital age presents complex challenges for states, international organizations, and civil society. Rapid technological advancement has amplified both the scope and scale of government surveillance, raising critical questions about proportionality, oversight, and accountability. At the same time, internet censorship and digital restrictions continue to limit access to information and constrain civic participation, particularly for vulnerable groups. Analytical engagement with these issues requires understanding the trade-offs between security, individual rights, and the public's right to information.

The international community has made strides through frameworks such as the UN Roadmap for Digital Cooperation, GDPR, and UN Human Rights Council resolutions, yet gaps remain in enforcement, standardization, and equitable implementation. Students should recognize that effective resolutions must balance these competing priorities by promoting mechanisms for judicial oversight, data protection, transparency, and inclusive access to digital spaces. Emphasizing human-rights-based approaches, capacity-building for states, and multilateral cooperation will be crucial in crafting policies that safeguard privacy and freedom of expression while minimizing potential misuse of surveillance technologies or overly restrictive content regulations.

Furthermore, integrating practical safeguards—such as clear limits on data retention, accountability for both governments and private actors, and avenues for redress—can strengthen compliance with international law and SDG 16. By critically assessing risks, gaps, and existing frameworks, students can propose resolutions that are both realistic and innovative, addressing the evolving challenges of digital governance and protecting fundamental human rights.

Questions to Address

1. How can governments balance national security with individual privacy rights online?
2. What measures can be implemented to protect freedom of expression online without enabling harmful content or misinformation?
3. How can the "right to be forgotten" and data protection regulations be harmonized with the public's right to access information?

Topic B: Combating Online Hate Speech and Protecting Children in Digital Spaces

Introduction

The expansion of digital platforms has significantly altered the landscape of communication, creating new opportunities for social interaction, education, and civic engagement. However, these platforms have also introduced risks, including cyberbullying, online hate speech, and the exploitation of children, which have implications for both individual rights and public safety. Children and adolescents are particularly vulnerable to harmful content, targeted harassment, and manipulative online algorithms, which can undermine their safety and development.[11]Statistics suggest that girls are twice as likely as boys to encounter online harassment in social media environments, highlighting the intersection of gender and digital vulnerability. For example, 32 % of teen girls reported experiencing two or more types of online abusive behavior compared with 24 % of teen boys in a U.S. survey.[12] AI-driven recommendation algorithms can unintentionally amplify harmful content, exposing children to repeated cycles of harassment and extremist material. Addressing these risks aligns with Sustainable Development Goal 5 on gender equality and SDG 16.2, which seeks to end abuse and exploitation of children, as evidence indicates that girls and marginalized groups are disproportionately affected by digital harassment.[13]

Efforts to address online hate speech and cyberbullying must balance the protection of vulnerable populations with the safeguarding of freedom of expression, consistent with international human rights frameworks. The United Nations Strategy and Plan of Action on Hate Speech emphasizes the need for multi-stakeholder approaches that include governments, civil society, and digital platforms to mitigate the dissemination of harmful content while preserving fundamental freedoms.[14] Similarly, UNESCO has highlighted the importance of media and digital literacy initiatives to enhance resilience and critical engagement with online content.[15] For instance, UNESCO's Digital Citizenship Education programs in over 25 countries train students to critically assess online content and report harmful behaviors**.**

[11] United Nations. (n.d.). *Child and youth safety online*. UN Global Issues. https://www.un.org/en/global-issues/child-and-youth-safety-online

[12] Pew Research Center, Teens and Cyberbullying 2022, December 15, 2022, https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/

[13] United Nations. (2023). *Press release: Guardrails urgently needed to contain "clear and present global threat" of online mis- and disinformation and hate speech*. https://www.un.org/sustainabledevelopment/blog/2023/06/press-release-guardrails-urgently-needed-to-contain-clear-and-present-global-threat-of-online-mis-and-disinformation-and-hate-speech-says-un-secretary-general

[14] United Nations. (2019). *United Nations Strategy and Plan of Action on Hate Speech*. https://www.un.org/en/delegate/addressing-hate-speech-digital-age

[15] United Nations. (n.d.). *International Day for Countering Hate Speech*. https://www.un.org/en/observances/countering-hate-speech

These approaches recognize that regulatory measures alone are insufficient and must be complemented by educational and preventive strategies. Combining legal regulation with algorithmic accountability ensures that harmful content is identified and mitigated without unduly restricting free expression. Protecting children from online risks remains a priority for the international community. Cyberbullying, grooming, and exposure to inappropriate or violent content can have long-term consequences for children's development and well-being. UN reports and policy briefs underscore the importance of coordinated legal frameworks, platform-level safeguards, and capacity-building programs for children, parents, and educators to reduce exposure to online harms.[16] [17] For SOCHUM, addressing these challenges requires a human-rights-based approach that balances protection from digital harm with the promotion of inclusive, participatory, and rights-respecting online environments.

Current Situation

Children's exposure to online risks, including cyberbullying, harassment, sexual exploitation, and hate speech, is increasingly documented as a concern for child rights and protection. According to the UN Special Representative on Violence Against Children, one in three internet users worldwide is under 18, and children face digital harms such as cyberbullying, unwanted sexual solicitation, and exposure to violent or discriminatory content.[18] National contexts reflect the global scale of this issue. In India, for example, the state of Karnataka recorded over 300 cases of cyberbullying between 2022 and 2025, with actions taken under provisions of the Information Technology Act targeting sexually explicit material involving minors.[19] In Malaysia, the Communications and Multimedia Commission received thousands of cyber harassment complaints between 2018 and 2019, demonstrating national mechanisms for reporting online abuse.[20] UNICEF reports that similar challenges exist in North Macedonia, where adolescents have reported exposure to harmful online content and participated in initiatives aimed at reducing cyberbullying and hate speech.[21]

[16] Special Representative of the Secretary-General on Violence Against Children. (n.d.). *Digital violence*. https://violenceagainstchildren.un.org/en/our-work/thematic-areas/digital-violence

[17] UNICEF & partners. (2025). *Protecting children from violence and exploitation in the digital environment: Policy brief*. https://www.unicef.org/media/164421/file/Policy%20brief_Protecting%20children%20from%20violence%20in%20the%20digital%20environment.pdf.pdf

[18] Special Representative of the Secretary-General on Violence Against Children. (n.d.). *Digital violence*. United Nations. https://violenceagainstchildren.un.org/en/our-work/thematic-areas/digital-violence

[19] United Nations General Assembly. (2023). *Protecting children from bullying, including cyberbullying* (A/RES/77/201). United Nations. https://digitallibrary.un.org/record/4092836/files/A_RES_77_201-EN.pdf

[20] United Nations. (2023). *Child and youth safety online: Global and national perspectives*. https://www.un.org/en/global-issues/child-and-youth-safety-online

[21] UNICEF. (2025, February 11). *Adolescents launch a movement for an internet free of cyberbullying and hate speech*. https://www.unicef.org/northmacedonia/press-releases/adolescents-launch-movement-internet-free-cyberbullying-and-hate-speech

States and international organizations have introduced preventive and regulatory measures to address these risks. In China, the Cyberspace Administration implemented *Operation Qinglang*, a campaign regulating online content deemed harmful to minors, including cyberbullying, inappropriate advertising, and media exposure.[22] Australia enacted legislation in 2024 restricting children under 16 from accessing major social media platforms, and several European countries, including France, Germany, and Denmark, have introduced age-based access restrictions or parental consent requirements for social media use.[23] However, critics note that age-based restrictions may be difficult to enforce online and could inadvertently limit educational and civic engagement opportunities for youth.

UN-backed programmes in the Western Balkans, including Albania and Bosnia and Herzegovina, have engaged youth in countering online hate speech and promoting inclusive digital spaces.[24] These examples illustrate the diversity of approaches in regulating digital environments while promoting child protection. Nonetheless, uneven implementation across regions points to the need for stronger international coordination and capacity-building.

Non-governmental and intergovernmental initiatives complement state actions in monitoring and mitigating online harms. UNICEF programs, such as the Global Kids Online project and Safer Internet Day campaigns, provide evidence-based interventions to reduce children's exposure to harmful content and engage young people in digital literacy and awareness programs.[25] [26] The UN Strategy and Plan of Action on Hate Speech emphasizes cooperation among Member States, technology companies, and civil society to address digital abuse while respecting freedom of expression.[27] The International Day for Countering Hate Speech also promotes global awareness and the dissemination of good practices to reduce online harassment and discrimination.[28] These programs operate alongside country-specific initiatives to address cyberbullying, radicalization, and exploitation, providing platforms for youth participation and policy implementation across diverse national contexts. However, disparities in digital access and enforcement capacity highlight ongoing challenges for equitable protection in all regions.

[22] Cyberspace Administration of China. (2022). *Operation Qinglang: Protecting minors online*. https://www.un.org/en/chronicle/article/operation-qinglang-protecting-minors-online

[23] United Nations. (2024). *Digital regulation and youth access: Case studies from Australia and Europe*. https://www.un.org/en/chronicle/article/digital-regulation-and-youth-access

[24] United Nations Peacebuilding Fund. (2023). *Nurturing safer digital spaces: Empowering youth against hate speech in the Western Balkans*. https://www.un.org/peacebuilding/zh/content/nurturing-safer-digital-spaces-empowering-youth-against-hate-speech-western-balkans

[25] UNICEF. (2025). *Protecting children in the digital environment*.

[26] United Nations. (2023). *Child and youth safety online*.

[27] United Nations. (2019). *United Nations Strategy and Plan of Action on Hate Speech*. https://www.un.org/en/delegate/addressing-hate-speech-digital-age

[28] United Nations. (n.d.). *International Day for Countering Hate Speech*. https://www.un.org/en/observances/countering-hate-speech

Conclusion

The proliferation of digital platforms has created important opportunities for learning, participation, and civic engagement, but it has also heightened children's exposure to online harms, including cyberbullying, harassment, sexual exploitation, and hate speech. These risks disproportionately affect girls, underscoring the gendered dimensions of digital vulnerability. Addressing such harms is not only a regulatory or technical challenge but a matter of protecting fundamental human rights, advancing gender equality, and ensuring that digital environments support the well-being and development of children.

While international frameworks such as the UN Strategy and Plan of Action on Hate Speech and Sustainable Development Goal 16.2 provide essential guidance, significant implementation gaps remain. Regulatory measures must be complemented by education, media and digital literacy, platform-level safeguards, and strengthened data protection. A coordinated multistakeholder approach involving governments, civil society, technology companies, and young people is essential to develop harmonized policies that safeguard children, respect freedom of expression, and advance equity, human rights, and sustainable development in the digital age.

Questions to Address

1. How can states protect children online without limiting freedom of expression?
2. Should governments focus more on regulation or education to prevent online harms?
3. How can UN frameworks support national policies while respecting sovereignty?
4. What role should digital platforms and civil society play in reducing online abuse?
5. How can policies address the disproportionate impact of online harms on girls and other vulnerable populations?