SUMMIT OF THE FUTURE INFORMATION CLEARINGHOUSE

BULLETIN NO. 5:

Headlines and Key Remarks from the Global Digital Compact Thematic Deep-Dives on "Data Protection" (24 April 2023) and "Human Rights Online" (8 May 2023)

PROJECT TEAM: Eliane El Haber and Mwendwa Kiogora *(Lead Authors, Bulletin No. 5)*, Eshana Amarasinghe, Fergus Watt, Ishaan Shah, Jebilson Raja Joslin and Jeffery Huffines

Global Digital Compact Thematic Deep-Dive –
Data Protection (24 April 2023)

Note: This bulletin summarizes the stakeholders remarks only (MS statements are not included).

ABOUT

The third thematic deep dive or informal consultations on the Global Digital Compact ([GDC](#)) was held on 24 April 2023 at the Trusteeship Council Chamber . "[The deep dives](#) aim to share knowledge and views, as well as allow for contributions on a wide range of digital issues". The Permanent Representative (PR) of Rwanda – H.E. Mr. Claver Gatete and PR of Sweden – H.E. Ms. Anna Karin Eneström are [Co-Facilitators](#) of the intergovernmental process negotiating the [GDC](#).

HEADLINES

There is a need to have data that is accurate, safe, accessible, and affordable. It should be up-to-date, standardized, and interoperable. Hence, this kind of data, which determines the way we live, should be highly protected.

RESOURCES

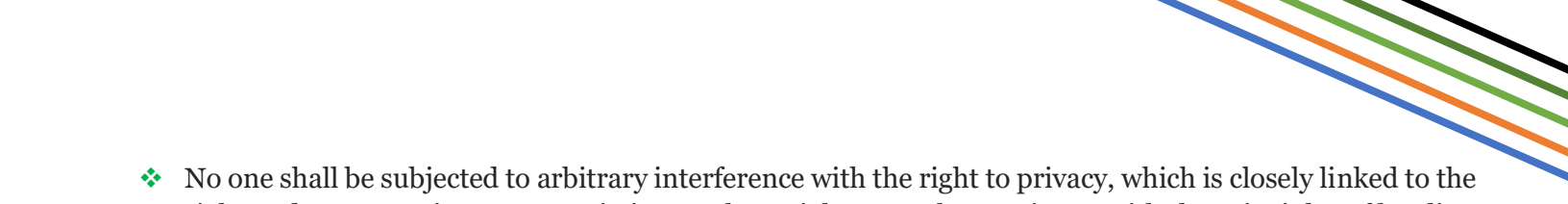1. [Letter from the Co-Facilitators – 18 April 2023](#)

STAKEHOLDERS REMARKS

Co-Facilitator	✚ Inviting all speakers to consider the following guiding questions, 1. [Art. 17 ICCPR](#) recognizes the individual right to privacy. How can governments, data protection authorities' private companies, the scientific community and civil society work together to ensure personal data is processed, stored, secured and protected against misuse? 2. What principles would support quality and interoperable data so that governments, international organizations, the private sector, civil society and individuals can contribute to and benefit from digital trade and economy and leave no one behind? 3. Data is a key enabler of innovation and research. How can stakeholders leverage tools such as (pseudo)anonymization, encryption, portability, etc. to drive innovation and interoperability while protecting personal data?

The stakeholders' remarks included contributions from but were not limited to [Google](#), [Microsoft](#), [Meta](#), [Youth IGF movement](#), [Association for Progressive Communications](#), [Bangladesh NGOs Network for Radio & Communication](#), [The Royal Society](#), [Digital cooperation organization](#), [Project Omna](#), [International Chamber of Commerce](#), [UNHCR](#), and [Caribbean Telecommunications Union](#).

❖ An increasing array of organizations use personal data to provide a growing range of services. Responsible data use can unlock benefits for people, companies, and other organizations around the world.

- [Google](#) has synthesized a set of high-level principles called the [Framework for Responsible Data Protection Regulation](#), which can be found online. These principles are based on established privacy regimes and are meant to apply to organizations that make decisions regarding the collection and use of personal information.
- There is a need to strengthen privacy and personal data protection Frameworks so that they effectively address the erosion of collective autonomy that arises from non-consensual data collection, individual and group profiling, recombination of third-party sharing, and downstream processing of anonymized personal data.
- There is a need to ensure that laws and policies for the economic government of data resources maximize social benefit and curtail the market tendency for the concentration of exploitation.
- Everyone has the right to the protection of data that concerns them and to be able to understand, in very simple terms, how that data is processed. No one shall be subjected to arbitrary interference with these rights, and any limitation of this right shall be reasonable, necessary, proportionate, and justifiable. Moreover, any processing of data shall be fair, lawful, and transparent, adhering to the data processing principles set out in international norms and standards.
- There is a need to preserve the robustness of encryption for sensitive data sharing, including end-to-end encryption, and promote the widespread use of end-to-end encryption. The competent operation of trustworthy digital systems relies on many fundamental security technologies including encryption, and these Technologies provide the technical assurance that enables people to entrust their data to digital systems.
- A billion people are online today. Protecting their data has never been more important in today's Digital World. Personal data is constantly collected, processed, and transmitted across borders. This data holds tremendous value and potential for digital trade innovation, research, and development, yet it poses significant risks to individual privacy and security if not handled and protected properly.
- [Microsoft](#) believes that privacy is a fundamental human right and that strong data privacy laws are vital for safeguarding it and building trust in technology. There is a need for strong data privacy laws that place accountability where it belongs, which is on the organizations that collect, store, and process data. As the number of privacy laws increases, so does the importance of interoperability.
- Clear, consistent rules across jurisdictions reduce complexity, promote accountability for responsible data practices, and help ensure that everyone's privacy is protected regardless of location.
- [Microsoft](#) believes the private sector should take data protection into account. Companies should be transparent about the data they collect and how they use it. There is a need for a right to privacy suited to protect women, girls, and other discriminated-against groups and marginalized people from new harms of abuse that are rooted in the patriarchal structures that fuel gender-based violence.
- The right to privacy in the digital realm is also about safety at its core. The right to privacy protects individuals from intrusion into their own or their family's personal lives by Third parties, creating an expectation of Privacy. That privacy can protect users online from sexual exploitation and abuse, such as having their personal and sexual information shared and distributed without their consent.
- Sharing data may bring many benefits. It has become necessary to share data for everyday tasks and engage with other people in today's society, but it is not without risks. Data can easily be exploited to cause harm and is especially dangerous for vulnerable individuals and communities, such as journalists, activists, human rights defenders, and members of oppressed and marginalized groups, which is why data must be strictly protected.
- The [GDC](#) process should employ a human-centric approach. Guided by the international human rights law framework as the basis for protecting such data.

- No one shall be subjected to arbitrary interference with the right to privacy, which is closely linked to the right to data protection; any restriction on these rights must be consistent with the principles of legality, necessity, and proportionality under international law.
- There is a need to adopt a new mentality regarding leadership, harm, and data harm prevention, so there is a need to advance a precautionary approach to data protection. There is a need to focus not only on the inputs and the nature of the data that circulates globally but also on the outcomes and the consequences for social groups. There is a need for robust and open methodologies for data protection impact assessment.
- Asylum claims must respect the confidentiality of Asylum information and regulate data sharing and access, particularly about countries of origin. Upholding the standards is vital to preventing risks for Asylum Seekers and ensuring the humanitarian nature of preservation.
- In the International Covenant on Civil and Political Rights , the Universal Declaration of Human Rights, and the Charter on Fundamental Rights of the European Union, they all established the right of every individual to maintain control over their data, as this is a precondition for the exercise of many other Freedom rights.
- The huge amount of data that's flowing over the internet is an important source of knowledge and economic power as it contributes and creates value to reach Sustainable Development Goals and also because data could be used for the benefit of humanity, but it is also used to provide users with information for marketing campaign purposes and also for malicious and surveillance purposes. That's why it's important and urgent to establish global principles and rules to protect data, regulate the collection, storage, and use of data, and ensure trust and safe transnational transfer of data. What is important is to strike the right balance between the use of data as an economic and social resource and data protection as a fundamental right of the individual. It is essential that data protection rights are guaranteed to protect the digital space and that the GDC includes this principle to defend this right.
- There is a need for governments to guarantee the processing, storage, and protection of their citizens data, placing the right to privacy at the center. There is also a need to analyze this issue from a gender perspective, taking into account that the dissemination of data does not affect all people in the same way.
- More than a billion people use Meta's applications every month, and in doing so, they have access to an interconnected world of people, ideas, news, communities, and commerce unconstrained by local or national boundaries. At its core, Meta wants to preserve an open, universally accessible internet with safety, security, and respect for human rights at its heart.
- While Meta is working to make progress, she should not be doing that alone. That's why Meta supports globally consistent regulations to set clear and fair rules for everyone and a safe and secure open internet where creativity and competition can thrive.
- The internet needs guardrails, not roadblocks. Many are drawn to the idea of digital sovereignty, whereby establishing digital walls at their National borders can better secure data generated by their citizens.
- Governments need to resist protectionist policies that do not further the protection against misuse of how personal data is processed, stored, secured, and protected. Instead, under such policies, the internet becomes a little less free and the digital economy becomes a little bit more constrained.
- It is essential to recognize that international human rights law acts as the basis for protecting the collection, processing, sharing, and use of personal data, which must be considered from the perspective of the younger generations.
- Young people are the generation that will be significantly affected by today's decisions. Today's youth are digital natives, living much of their lives online, and therefore have found the most critical spheres of their lives digitalized. With this digitalization comes a heightened risk and increased vulnerability to

cyberattacks for young people. Their data is an extension of themselves, personal and private, yet beyond their control.

❖ As the world continues to leverage data as an enabler of innovation and research, it is crucial to prioritize the protection of personal data, ensuring its use is transparent, responsible, and beneficial to all. Innovation and research are essential drivers of progress, yet they must not come at the expense of personal data protection.

❖ Young people are concerned by the absence of governance and laws concerning digital spaces and data protection. Governments must enact more legislation to incentivize companies to invest in cyber security and treat data responsibly and ethically.

Global Digital Compact Thematic Deep Dive:

Human Rights (8 May 2023)

ABOUT

The Global Digital Compact (GDC), proposed in the UN Secretary General's [Our Common Agenda](#) report, aims to establish principles for an 'open, free, and secure digital future'. The third thematic deep dive on the GDC on Human Rights Online was held on 8 May 2023, in a hybrid format (online and in-person at the UN Headquarters in New York). The Co-Facilitators of the intergovernmental process negotiating the GDC - H.E. Ms. Anna Karin Eneström, Permanent Representative (PR) of Sweden and H.E. Mr. Claver Gatete. PR for Rwanda moderated the session. At the beginning of the deep dive, United Nations High Commissioner for Human Rights Volker Türk and Najat Maalla, the Special Representative of the Secretary-General on Violence against Children, set the stage for the deep dive. Member State (MS), Intergovernmental agencies, private sector and civil society representatives made their interventions after the briefings

HIGHLIGHTS

KEY AREAS DISCUSSED	VIEWS OF MS
Protection of Human Rights in the Digital Sphere	There is a growing recognition of the need to protect human rights in the context of the digital space. Discussions often revolve around the challenges and opportunities posed by emerging technologies and the internet, with an emphasis on ensuring that human rights, such as freedom of expression, privacy, and non-discrimination, are upheld online.
Balancing Rights and Responsibilities:	Member states and stakeholders are grappling with the task of striking a balance between protecting human rights and addressing the potential risks and harms associated with the use of technology and the digital space. This includes discussions on combating hate speech, disinformation, and online harassment while safeguarding freedom of expression and privacy rights
Data Privacy and Protection	Discussions often center around the importance of strong data protection frameworks, consent mechanisms, and accountability measures to ensure that individuals' personal data is handled responsibly and securely.
Digital Divide and Inclusion	This involves promoting equal access to digital technologies, addressing disparities in internet access, digital literacy, and technological infrastructure to ensure that all individuals have the opportunity to benefit from the digital economy
Online Freedom of Expression and Censorship	Discussions were on how to balance between protecting freedom of expression and addressing issues of online censorship and content regulation. Member states and stakeholders explored ways to

	foster an open and inclusive digital environment that respects diverse perspectives while addressing harmful and illegal content.
Ethical Use of Technology	There is increasing recognition of the ethical implications of technological advancements. Conversations often focus on the responsible and ethical use of technologies such as artificial intelligence (AI), surveillance systems, and biometrics, ensuring that they do not infringe upon human rights or perpetuate discrimination.
Multi-stakeholder Collaboration	Stakeholders emphasized the involvement of governments, civil society organizations, technology companies, a challenges in the digital space. Collaborative efforts are seen as vital for developing comprehensive policies, regulations, and guidelines.

HEADLINES

Digital technologies can greatly contribute to the protection of human rights. However, digital surveillance, censorship, algorithmic bias, online harassment, and other forms of abuse can suppress or violate human rights. The following are the guiding questions provided by the Co-facilitators to guide the discussions:

- How can women and girls, children, and persons in vulnerable situations such as persons with disabilities or persons belonging to linguistic minorities be supported in exercising their human rights online?
- What are the gaps in terms of existing mechanisms for protection and promotion of human rights in the digital domain?
- How can accountability of digital platforms - public and private - be strengthened?
- How can international organizations, Member States and other stakeholders work together to ensure human rights offline are protected online?

RESOURCES

1.Letter from the Co facilitators - 2 May 2023

2. UNSG's Roadmap for Digital Cooperation Ensuring the Protection of Human Rights

3. Policy Brief : Global Digital Compact: An Open, free and

4. Secure Digital Future for All

MEMBER STATES STATEMENTS

1. Colombia
2. European Union
3. UN High Commissioner for Human Rights

MEMBER STATES REMARKS

Member State	Interventions
European Union	- Good civil and political rights as well as economic, social, and cultural rights should be the starting point. Technology should strengthen and protect these rights, not weaken them. - Rapid development of digital technologies has brought many benefits, including improved communication and access to public services. - Technologies can be drivers of misinformation and can be misused to spread disinformation, hate speech, violate privacy, increase surveillance, and perpetuate harassment, violence, discrimination, and inequalities. - Marginalized communities, women, and girls are disproportionately affected by online sexual and gender-based violence and disinformation. - Robust measures are needed to prevent, detect, address, criminalize, and end online sexual and gender-based violence. - Children are at significant risk of exposure to online threats and require targeted prevention initiatives. The EU prioritizes the protection, empowerment, and respect of children online and supports digital accessibility and closing digital divides. - The EU condemns all kinds of Internet shutdowns, information manipulation, interference, and disinformation and is committed to digital privacy, data protection, and the promotion of digital humanities and humanism. - A multi-stakeholder approach involving national authorities, human rights institutions, academia, civil society, human rights defenders, journalists, international and regional organizations, and the private sector is necessary. - A systemic approach is needed, considering the entire cycle of digital technologies, including their design, development, deployment, evaluation, and use. - Online environment should be safe from discrimination, harassment, cyberbullying, online sexual and gender-based violence, information manipulation, hate speech, and harmful content. - Privacy, data protection, civil society space, and combating mass surveillance, internet shutdowns, and online censorship are crucial. - Equal opportunities for women and girls to access, use, lead, and design technology should be ensured by addressing gender dimensions of digital inequality, promoting inclusive innovation ecosystems, and addressing the root causes of gender inequalities.
Pakistan	- Online platforms and social media companies have a shared responsibility to ensure their practices align with international human rights law and prevent the spread of disinformation. - UNGA Resolution 76-227 can provide useful guidelines for addressing disinformation comprehensively and the Geneva Declaration of principles' balanced approach to human rights should guide discussions in the compact. - The right to development should be reaffirmed as the overarching framework for discussions, considering the 2.7 billion people who remain offline, are mainly in developing countries. - Bridging the digital divide requires a supportive international environment, including FDI transfer of technology, international cooperation, and the participation of developing countries in global decision-making. - Adverse impacts of international intellectual property protection regimes on countries' rights, particularly in accessing life-saving technologies, should be examined.

	• A compact incorporating human rights should recognize the centrality of the right to development.
Denmark	• A GDC should be developed as part of an international rule-based order, rooted in human rights. • Trustworthy technology requires a holistic, inclusive, and human rights-based approach throughout its life cycle. • Access to digital spaces is limited for many due to connectivity issues and deliberate censorship. • Governments and regulators have a duty to protect human rights and regulate technological advancements. • Mindful progress is needed, seeking guidance from civil society and constructive partnerships with the private sector. • Multi-stakeholder collaboration is crucial to bridge knowledge gaps and address challenges in the digital space. • Strong guardrails should be developed to tackle information manipulation, harassment, surveillance, and ensure accountability. • The UN guiding principles on business and human rights provide a foundation, and collaboration with civil society and the private sector is important.
Argentina	• The safety of people is at risk due to new forms of crimes and malicious use of networks. • The digitalization accelerated by the COVID-19 pandemic has increased vulnerabilities. • Digital citizenship and skill development are necessary for responsible use of digital environments. • Prevention and protection from various forms of violence in digital environments, particularly towards children and adolescents, are crucial. • International cooperation and dialogue are needed to mitigate the malicious use of ICTs. • Bridging digital gaps and articulating mechanisms are necessary for states to fulfill their role in guaranteeing rights in civil states. • Preventive work and awareness campaigns are vital to address threats to people's rights, especially vulnerable groups. • Maintaining a free, open, resilient, peaceful, and safe civil space is imperative. • ICTs should be used in compliance with the principles of the UN Charter and international human rights law.
Bangladesh	• Pervasive tracking of internet users by various entities poses threats to privacy and human rights. • Individual autonomy is at risk, as algorithms dictate personal decisions and opportunities, even in democratic societies. • People in least developed countries and marginalized/vulnerable groups face greater barriers to connectivity, privacy violations, and online insecurity. • A technology governance and architecture are needed to ensure online safety, privacy, inclusion, and human rights protection. • Expanded legal frameworks based on human rights approaches must be developed, and privacy laws should be enacted and enforced in compliance with international standards. • Content governance measures should protect data privacy, freedom of expression, ensure affordable access, and address illegal and harmful online content.

	• Protection against unlawful or unnecessary surveillance, including restrictions on encryption technology and surveillance of the public, must comply with international human rights law. • Tech companies, social media platforms, ad firms, and businesses must adopt safeguards to protect privacy rights and digital identity, as well as prevent the spread of hate speech, misinformation, and discrimination. • The GDC must aim to reverse the negative impact of technology on safety and freedom, making technology a tool for freedom and safety
Brazil	• Brazil advocates for an open, secure, accessible, and peaceful cyberspace governed by international law, including human rights law. • There are interlinkages between freedom of expression and other human rights, emphasizing the need for appropriate safeguards to protect all rights. • Protection of rights and privacy online is essential for people to engage in economic, social, political, and cultural activities with confidence. • There is need for a broad human rights perspective, ensuring protection against violations, universal connectivity, digital inclusion, and the right to development as enablers of human rights enjoyment online and offline.
Canada	• Digital technologies are a powerful catalyst for sustainable development and advancing human rights. • Commitment to protecting and promoting human rights online and across the digital ecosystem. • The global digital compact should clearly outline fundamental principles and safeguards for advancing human rights. • Commitment to refraining from misusing or abusing the internet, digital technologies, data, and algorithmic tools. • Focus on securing individuals' privacy, maintaining secure and reliable connectivity, and promoting a free and competitive global economy. • Working with global partners to update and establish shared principles in the area of human rights online. • Addressing technology-facilitated gender-based violence as a critical human rights and digital security priority. • Recognition of the importance of online access and access to information for human rights. • Advocacy for an open, free, global, interoperable, reliable, and secure internet. • Human rights-based and multi-stakeholder approach to the development and use of digital technologies. • Emphasis on the right to freedom of expression and information as an enabler of other human rights. • Regulation of digital platforms for information should prioritize minimizing restrictions on freedom of expression and apply the least intrusive measures possible. • Protection of privacy on digital platforms is essential to protect freedom of expression and information. • Support for shaping global norms to protect and promote human rights online. • Engagement in existing UN efforts and welcoming the GDC process's emphasis on human rights online.
China	• The rapid development of digital technology has greatly contributed to people's well-being.

	• The discussions on online human rights should coordinate with other relevant processes at the UN to avoid duplication. • Digital divides between and within countries are widening, and efforts should be made to ensure inclusivity and development globally. • Support should be provided to developing countries for digital infrastructure and capacity building to ensure equal access and benefits of digital technology. • Politicizing human rights issues should be opposed, particularly actions that impair critical infrastructure, impose surveillance, and unauthorized data collection. • National differences and diverse paths to realizing human rights should be respected, considering the special conditions and levels of development of each state. • China has enacted laws and regulations on personal information protection and is willing to communicate and dialogue with relevant parties to explore approaches for harnessing emerging technologies for the well-being of all.
Colombia	• Governments should provide relevant tools, knowledge, and capacities to ensure the rights of women, girls, young people, children, indigenous peoples, older persons, and persons with disabilities are protected online. • Users must understand and exercise their right to privacy and data protection to prevent violence, discrimination, and harassment in the digital sphere. • The digital revolution should prioritize offering quality education and accessible digital materials for schools and students at all levels. • Intersectional approach should be adopted in the development and use of digital platforms, algorithms, and artificial intelligence to avoid perpetuating stereotypes and discriminatory structures. • The GDC should create a feminist digital environment that respects diversity and traditional knowledge. • Measures addressing internet governance, data flows, misinformation, and artificial intelligence should align with international law and not compromise human rights, freedom of speech, privacy, and access to information.
Cuba	• ICT should be consistent with international peace and security objectives. • The social impact of new technologies and their values should be considered, since historical, cultural, and legal values and traditions can be impacted by technological change. • Urgent action is needed to counter cyber threats and attacks on computer systems. • The call for a negotiation process within the UN to adopt legally binding international instruments for cybersecurity. • The need for democratic and participatory internet governance based on the UN Charter and international law. • There is a need for recognition of states' sovereign right to regulate public policy issues.
Dominican Republic	• Transparent, robust, and inclusive policies and practices are needed to strengthen accountability of digital platforms and address concerns related to data breaches, surveillance, and unauthorized access to personal information. • The involvement and participation of users, including children, youth, women, persons with disabilities, and those in remote areas, is essential to consider the impact on their rights online. • Focus on educating children about the digital environment and developing user-friendly digital tools is crucial for enhancing child protection online.

	• Women's rights online require attention due to unique forms of harassment, violence, abuse, and discrimination they face, including gender biases in algorithms.
	• Bridging the digital gender divide, protecting privacy and data, and promoting women's representation and participation are vital for empowering women and achieving gender equality.
	• Digital platforms and technology companies have a responsibility to ensure fair and unbiased algorithms, content recommendation systems, and user interfaces.
	• Governments and online platforms must create safe and inclusive spaces that actively combat hate speech, misinformation, discriminatory content, and online abuse, with mechanisms for reporting and appropriate actions against offenders.
Egypt	• ICTs, global interconnectedness, and technological innovation have the potential to bridge the digital divide and build knowledgable societies.
	• Intellectual property protection regimes can inadequately impact the right to enjoy the benefits of scientific progress and culture.
	• Human rights in the digital sphere extend beyond freedom of expression, speech, and privacy to preventing misuse that violates human rights.
	• Misuse of digital platforms leads to the dissemination of misinformation, criminal activities, extremist ideologies, and hate speech.
	• Unpunished actions endanger societal peace and the rights of migrants, refugees, and minorities, including Muslim minorities.
	• Balancing the right to freedom of expression (Article 19) with the prevention of incitement to hatred and violence (Article 20) is crucial.
	• States have the primary responsibility to establish laws, regulations, and ethical codes to govern the digital space, ensuring accountability and remedies for victims.
	• The GDC should recognize the right to development, establish safeguards against criminal use of digital content, and expand exceptions to intellectual property laws to promote digital access and transfer of related technology
Finland	• We advocate for an open, free, and secure internet that is safe for all, including women, girls, children, and vulnerable individuals.
	• Ensuring the same human rights online and offline, including protection of personal data and privacy.
	• We should endeavor to connect people to the internet and addressing digital inequality to enhance economic inclusion, democratic participation, and equitable digital development.
	• Internet fragmentation poses risks to sustainable development, universal human rights, international trade, and stability.
	• GDC should uphold a global, free, open, interoperable, secure, and reliable internet, while strengthening the multi-stakeholder model for internet governance.
	• We have an opportunity of bridging the gender digital divide, with active participation in the Generation Equality initiative and addressing online gender-based violence.
	• Digital technologies have the potential to improve democratic governance and citizen participation, but misinformation and erosion of trust pose challenges.
	• High-quality education, media literacy, and critical thinking are vital tools to combat misinformation.

	• Stakeholders, including civil society, play a crucial role in promoting digitalization and protecting human rights. • Protecting the work of human rights defenders in the digital sphere is a priority. • The UN plays a role in promoting a rules-based cyberspace and prioritizing cybersecurity based on respect for human rights. • Developing common understandings on how international law, including international humanitarian law, applies in the cyber context should be a key focus of the GDC.

Indonesia	• Challenges to human rights online include the borderless nature of the internet, different regulations between countries, and the digital divide.
	• Three proposed points for the GDC:
	⁜ Fostering dialogue on human rights online to share knowledge and best practices.
	    • Ensuring the protection and promotion of activities in the digital space with a human rights-based approach, including addressing data theft, exploitation, hate speech, discrimination, and harmful online content.
	    • Empowering education and awareness-raising initiatives in digital literacy to bridge the education gap, provide access to educational resources, and promote responsible use of the online space.
	• Collaboration and involvement of multiple stakeholders are necessary for protecting and promoting human rights in the digital domain.

Iran	• States have the right to operate their own cyberspace according to their national laws and regulations. • States should have the necessary tools and capacities to exercise sovereignty in cyberspace to protect their civilian systems and digital resources. • Each country has the right to choose its own digital development model and determine policies for connectivity, access, and management based on domestic laws and culture. • Big tech companies and cross-border platforms should have transparent privacy policies that align with the laws and cultural values of the countries where they operate. • GDC should reject digital colonialism, unilateralism, and adhere to fundamental values such as human rights, cultural diversity, development justice, equality, non-discrimination, and security. • Users' rights should be respected, considering digital literacy, and efforts should be made to create a safe, healthy, and ethical online space, especially for children and students. • Digital technologies, including AI, should refrain from misusing or abusing the internet, data, algorithms, or any other tools that pose serious challenges to countries and public interest. • All stakeholders in the ICT environment should observe responsible behavior, adhere to principles, rules, and regulations, and be accountable for their actions, especially during global crises and pandemics. • The GDC should work towards creating an inclusive, equitable, and accessible digital ecosystem for all, facilitating technology and knowledge transfer to support sustainable development and global access.
Mexico	• Digital technologies have high value for achieving sustainable development, but they can also be used to violate human rights.

	- Concerns include illegal use of surveillance technologies, proliferation of misinformation, cyberbullying, racism, xenophobia, hate speech, and gender-based violence. - Human rights offline must be protected online, ensuring promotion, respect, and fulfillment of human rights in the development and regulation of digital technologies. - Human rights should be at the center of regulatory frameworks and legislation, particularly for emerging technologies. - Gender transformative approaches should be applied in the design, development, and application of digital technologies, promoting an open, secure, accessible, and affordable environment for women, adolescents, and girls. - The transformative potential of the global digital pact depends on a human rights perspective for the benefit of all people.
Romania	- Digital technology is seen as the "wild west" for human rights, emphasizing the need for accountability and safeguards. - Violations such as privacy breaches, data protection issues, online surveillance, and censorship undermine democracy and human rights. - Children are spending more time online, facing risks such as cyberbullying, peer-to-peer violence, sexual exploitation, and targeted marketing. - Digital and mental health are priorities for youth, and the Global Digital Compact should address these issues. - The GDC should support digital education, enhance digital skills, raise awareness of misinformation, and ensure the right to express opinions safely. - Inclusive debates should be free from xenophobia, racism, harassment, bias, and bullying. - AI also requires safeguards to prevent misinformation, abuse, and infringement on human rights.
Russia	- There is no consensus on the applicability of human rights in the digital realm. - There is no consensus with the statement that human rights are applicable online and offline. - We agreement on the need to protect children from bullying and violence online. - Emphasis on the need to consider the international covenants on civil, political, economic, social, and cultural rights. - There is a lack of rational explanation on how important human rights can be recognized or realized online. - Call to discuss a broader range of human rights in the context of the global digital landscape. - Welcoming the participation of private corporations and digital platforms but emphasizing the need for their accountability. - States have the primary responsibility to promote and protect human rights, unlike private corporations.
Spain	- Digital rights will be a prominent priority during Spain's presidency of the European Union Council from July to December 2023. - The Spanish government adopted a charter on digital rights two years ago to protect citizens' rights in the internet and artificial intelligence era. - The charter's purpose is to enhance citizens' rights, instill confidence, and foster trust in technology. It acts as a reference for legislative initiatives and public policies, encompassing fundamental rights, public engagement,

	workplace social rights, and digital rights in areas such as artificial intelligence and neural ethics. • Measures are in place to ensure the effectiveness and respect of these rights through administrative and judicial remedy. • The GDC should prioritize human rights in international governance and provide guidance on human rights standards in the digital age, promote human rights-based regulatory frameworks, and ensure online safe spaces and transparent and accountable content governance frameworks.
Singapore	• It is crucial to steer clear of polarizing and divisive debates based on geopolitical lines and instead establish a shared understanding among member states on how to navigate their differences and disagreements. • It has to be recognized that different states have the sovereign right to determine their own approaches based on national circumstances and level of development. • Access to the internet is still a significant issue, with a large portion of the global population lacking connectivity
South Africa	• Need for relevant local language and child-friendly content on online platforms. • Provision of educational and awareness material in accessible formats, including for persons with disabilities. • There are gaps in existing mechanisms for protecting and promoting human rights in the digital domain. • Addressing inconsistencies in the definition of a child and aligning it with existing mechanisms. • Specialized training for law enforcement, prosecutors, and judges on human rights abuses and violations online. • Importance of international cooperation to combat online crimes and share best practices. • Utilization of existing tools and instruments, such as UNESCO recommendations on ethics in artificial intelligence and general comments on children's rights in the digital environment.
South Korea	• Digital technology should contribute to promoting universal values of freedom, solidarity, and human rights. • Efforts should be made to create a safe digital environment and ensure digital accessibility for everyone. • Tech-facilitated violence, such as online gender-based violence and hate speech targeting vulnerable groups, should be addressed. • Infringement of individual freedom and human rights due to the abuse of digital technology by state powers should be recognized and responded to. • Responsible behavior by private actors and the development of technology ethics should be encouraged. • A multi-stakeholder model is necessary to effectively protect and promote human rights in the digital age. • Human rights norms should be integrated into all stages of technology development and commercialization. • Collaboration between the tech community and the human rights community is crucial.
Switzerland	• Global connectivity should go beyond access to the internet and be inextricably linked to safeguarding human rights online. • Human-centered and respectful development and deployment of new technologies require an open and inclusive multi-stakeholder process.

	• Companies using new technology should implement human rights due diligence and address adverse human rights impacts. • Effective remedies should be available to individuals and communities exposed to human rights risks online. • Governments have a duty to guarantee freedom of expression and protect fundamental human rights, including protection from discrimination. • A clear framework for communication on digital platforms should be developed and applied, with measures to combat hate speech and disinformation consistent with international law and human rights protection. • The development and use of digital technology should be guided by UN guiding principles on human rights and business and human rights. • The work of the Freedom Online Coalition can inform the content of the Global Digital Compact on human rights.
United Kingdom	• The UK is committed to a multi-stakeholder model for maximizing the benefits of the internet and digital technologies. • GDC is crucial in shaping a collective approach that supports human rights and enables inclusive participation in the digital space. • The internet and digital technologies offer opportunities for sharing thoughts, accessing information, coordinating action, and accessing education and healthcare online. • Digital technology plays a significant role in documenting and investigating human rights violations and abuses, driving accountability efforts; however, there are complex risks associated with the online world, including targeted persecution, gender-based violence, and restrictions on freedom of expression. • Internet shutdowns and restrictions can severely impact human rights and democratic engagement. • The UK is actively addressing these challenges through its membership in the freedom online Coalition. • Businesses also have a responsibility to respect human rights throughout their operations.
USA	• Digital technologies are a powerful catalyst for sustainable development and advancing human rights. • GDC should clearly outline fundamental principles and safeguards for advancing human rights. • Focus on securing individuals' privacy, maintaining secure and reliable connectivity, and promoting a free and competitive global economy. • Working with global partners to update and establish shared principles in the area of human rights online. • Recognition of the importance of online access and access to information for human rights and advocate for an open, free, global, interoperable, reliable, and secure internet. • Regulation of digital platforms for information should prioritize minimizing restrictions on freedom of expression and apply the least intrusive measures possible. • Protection of privacy on digital platforms is essential to protect freedom of expression and information. • Support for shaping global norms to protect and promote human rights online.

Stakeholder Remarks

- Human rights must be protected online, just like in the physical world, as it is essential to ensure an inclusive, safe, ethical, and prosperous digital economy. This requires a commitment to the protection and promotion of digital rights through coordinated global efforts, including collaboration with member states, partners, and observers.

- We all have a collective responsibility to safeguard fundamental rights, dignity, autonomy, security, and freedoms in the digital age.
- Discrimination in the digital public sphere based on social locations such as class, race, gender, and caste poses threats to human rights, particularly for women and marginalized groups.
- There are concerns about the rapid development of digital technologies without accompanying legislation, services, and education
- The COVID-19 pandemic has highlighted issues of digital security, privacy, freedom of expression, and further marginalization of vulnerable communities.
- Need to create a digital safe space and protect people's rights online.
- Focus on multi-stakeholder dialogues and mobilizing resources to address digital rights issues.
- Acknowledgment of the digital connectivity gap and the need for affordable access and digital literacy for all.
- Barriers to digital participation: cost-prohibitive access and insufficient digital literacy
- Focus on algorithmic bias resulting from the model, algorithm design, or data sets. Only around 22% of women are in AI, and equal representation is urgent to avoid biased algorithms.

- The proliferation of non-binding AI principles and ethical guidelines worldwide has been a positive step towards addressing the ethical implications of artificial intelligence. However, these principles and guidelines alone are insufficient in tackling the pressing issue of algorithmic bias.
- To effectively address biases and discrimination, there is a need for specific binding rules that govern AI systems.
- Current rules should be reviewed and, if needed, new regulations implemented to ensure online protection of human rights, fostering fairness, accountability, and transparency in AI technology development and deployment.
- Highlighting areas such as universality of the internet, privacy protection, rights of vulnerable groups, internet as a tool for education, and using digital capabilities to promote human rights and contribute to the Sustainable Development Goals.
- Governments and companies both have roles in conducting human rights due diligence and impact assessments when regulating or deploying digital technologies.
- Incorporating stakeholder consultation is essential for regulating and deploying digital technologies, as the practical implementation of international human rights laws necessitates multi-stakeholder dialogue and collaboration. Through knowledge sharing and collaborative efforts, we can shape the use of digital technologies in a way that protects and advances human rights.
- Technology companies are guided by internationally recognized human rights standards, such as the Universal Declaration of Human Rights and the UN Guiding Principles on Business and Human Rights.
- Governments need to invest in improving global connectivity for all people.
- GDC should build upon existing frameworks, multi-stakeholder efforts, and voluntary initiatives to promote internationally accepted standards for human rights.

Children:
- Emphasis on addressing child protection issues in digital environments.
- High prevalence of online sexual abuse among internet-using children, particularly in low and middle-income countries.
- Collaboration between technology sector, civil society, governments, and children for online safety and children's rights.
- Emphasis on the need for child protection, addressing issues such as sexual exploitation, violence, economic exploitation, and recruitment on the internet.

- Ensuring children's access to justice and remedies for rights violations in digital environments.
  - Prioritize the best interests of every child in the provision, regulation, design, management, and use of digital technologies.
  - Update and enforce legislation to protect children from violence and exploitation in digital environments.
  - Businesses should respect children's rights, conduct child rights due diligence, and support child well-being through digital products and services.
  - Ensure children's access to justice and remedies for violations of their rights in digital environments.
  - Base policies and interventions on updated data and research, including assessing how national systems respond to technology-facilitated crimes against children.

Gender and vulnerable groups
- Limited internet connectivity remains a challenge for nearly a third of the global population, especially vulnerable populations.
- GDC and member states' involvement in advancing gender equality in the algorithmic age are crucial so as to to integrate a gender transformative perspective into AI and recognize the significant role of women in AI development
- A global approach is necessary to address gender equality in the realm of AI. Unfortunately, technology is being exploited by malicious state and non-state actors to harm and suppress vulnerable groups.
- To ensure safety and security, internet governance efforts should incorporate gender and diversity-responsive procedures and regulations.
- Importance of universality of the internet, privacy protection, rights of vulnerable groups, and using digital capabilities for education.