

EuroSSIG
Summer School on Internet Governance

Global Digital Compact

Follow up statement by the fellows of the European Summer School on Internet Governance (EuroSSIG) 2023

focussing on Policy Brief 5 'A Global Digital Compact – an
Open, Free and Secure Digital Future for All' published in
May, 2023

Meissen, October, 2023



Overview

In 2022 Fellows submitted a [statement](#) on the proposed “Global Digital Compact”. This submission is a follow up to that statements with a specific focus on Policy Brief 5 ‘**A Global Digital Compact – an Open, Free and Secure Digital Future for All**’ published in May, 2023.

The Fellows in 2023¹ were invited to pick a few (2-4) of the themes discussed in the UN Secretary-General’s Brief for discussion and consideration. They picked the following areas for comment

- Theme 3: Upholding Human Rights
- Theme 4: An inclusive, open, secure, and shared internet
- Theme 6: Data protection and empowerment
- Theme 7: Agile governance of AI and other emerging technologies

The comments about each theme are structured along the following aspects: considerations and comments about the subject, concerns (if any) in relation to Policy Brief 5, and suggestions.

In several cases the comments this year build on the comments made in 2022 by that year’s fellows; when this is the case, the document quotes the 2022 submission.

1 The explanation of the exercise can be found in https://docs.google.com/document/d/1dTU1z5yDeFFQBD4H_fkKJA1Zsp48tX1eVYPBm40dw0E/edit?usp=sharing

Table of Content

Overview	2
Thematic comments	
Theme 3. Upholding human rights	4
Considerations and comments	
Concerns	
Suggestions	
Theme 4. An inclusive, open, secure, and shared internet	6
Considerations and comments	
Concerns	
Suggestions	
Theme 6. Data protection and empowerment	8
Considerations and comments	
Suggestions	
Theme 7. Agile governance of AI and other emerging technologies	10
Considerations and comments	
Suggestions	
Fellows participating in preparing the statement	12

Thematic comments

Theme 3. Upholding human rights

Considerations and comments

The international community should work towards upholding human rights in digital spaces through agreements, legislation and partnerships. The same rights offline must also be protected online for ensuring dignity and security of individuals and communities.

We welcome that access to the internet is already included in human rights conventions under article 19 on Access to Information. Access to the internet facilitates the attainment and realisation of human rights. To ensure this for everybody, and especially women and marginalised communities², meaningful connectivity should be incorporated into existing human rights frameworks on social, civil, political, economic, and cultural rights.

The Global Digital Compact should use the Sustainable Development Goals (SDGs), which are inextricably linked to basic human rights in all areas, as a basis of its principles. The focus on the individual goals and targets related to the internet and new technologies should be strengthened through targeted interventions and investments.

Concerns

- We are concerned that UN bodies that work on digitalisation, new technologies and internet governance frequently lack effective coordination and efficient information-sharing mechanisms. This leads to missed opportunities for cooperation and, in some cases, duplication of efforts. The situation is exacerbated by ineffective tracking and monitoring of digital interventions of multiple development agencies working in the same domain.
- Furthermore, we are concerned by the abuse of personal data by state and non-state actors, infringing upon human rights (for example, in cases of surveillance technology, arbitrary prosecutions, and technology-facilitated gender-based violence).
- The Policy Brief #5 is lacking a distinct call-to-action for all stakeholders - private sector, public sector, technical community, academia and civil society - to do their part in upholding and furthering human rights online. It remains unclear how accountability of (and to) involved stakeholders can be ensured.
- We are also concerned that there is not enough protection against persecution, censorship, and abuse for human rights defenders, civil society organisations, and academia that work on digital human rights issues.
- We are concerned about the lack of protection for women in politics and LGBTQI+ people in politics.

² Marginalized communities that need a special focus are LGBTQI+, indigenous, disabled, poor and displaced people as well as religious minorities and BiPoC communities.

Suggestions

- The Office of the Secretary General's Envoy on Technology should further coordinate among UN bodies in the field of digital technologies to ensure coherence and avoid duplication of efforts.
- In addition, all development agencies should share and learn from knowledge and capacity fora.
- The Private Sector should be held accountable (together with other stakeholders) for content moderation of discriminatory text and imagery on their platforms, as well as data and privacy protection. It should also implement a process for reporting GBoV as well as capacity building on gender based online violence (GBoV) and other forms of discrimination for staff that work on codes, algorithms and content moderation.
- The Public Sector and Member States should set up national laws to uphold data, privacy and human rights protection as well as labor rights.
- Member States and UN bodies should work towards regulations that protect children online from child abuse in its many forms including: exploitation, grooming, the dangers and abuse of social media use, and the impact of new technologies on children's physical and mental health. These measures should respect and take into account the rights of children enshrined in the International Convention on the Rights of the Child.
- The ILO, with Member States, should develop guidelines to protect the rights of platform workers in the gig economy.
- The GDC should put a particular focus on the regulation and safeguarding of human rights in the face of AI and other emerging technologies.
- The Member States should ensure cyber harassment laws are not misused.
- All stakeholders should work towards a more collaborative approach to deal with Technology Facilitated Gender-Based Violence and capacity building of law enforcement agencies that deal with GBoV.
- Member States and the private sector should commit to targeted investments for internet infrastructure and creating public-private partnerships to reach areas of true access gap in working towards bridging the digital divide with a special focus on rural broadband connectivity as well as meaningful access.
- UN bodies should increase the diversity of stakeholders funded for UN interventions, such as civil society organizations and improve standardized assessment of the impact of UN bodies' work.
- The GDC should address *threats of censorship and to the media by State and non-State entities*.

Theme 4. An inclusive, open, secure, and shared internet

Considerations and comments

An inclusive, open, secure, and shared Internet cannot be achieved if the technical infrastructure of the Internet is fragmented. Therefore, we reaffirm the following statement from the submission by the fellows of the 2022 European Summer School on Internet Governance (EuroSSIG) (page 6):

“Core Principles

- 1. The Internet, being a network of networks, must remain interoperable.*
- 2. It is crucial that we, as a global community, preserve the integrity of the Internet.*
- 3. The Internet must remain globally reachable through a unique identifier system.*
- 4. Internet openness is vital as it allows to achieve potential benefits for all.*
- 5. The efforts to prevent Internet fragmentation should take place simultaneously on three levels: on the technical layer, the regulatory layer, and socio-economical layer.*

The interoperable and globally reachable Internet, as we have known it since its origin, has enabled enormous network effects. The positive impact on socio-economic development, citizen participation, access to information and all kinds of digital services has completely changed our societies. Preserving a single, interoperable, open and globally reachable Internet is therefore in the global public interest.”

We affirm the value of bottom-up multistakeholder processes like ICANN that facilitate the participation of core stakeholder groups (including the technical community, civil society, industry and the public sector) to address issues related to Internet governance.

Concerns

- The Policy Brief 5 references the reinforcement of multistakeholder governance of the Internet, but it also suggests the establishment of an additional forum - the Digital Cooperation Forum (DCF) – which may weaken the effectiveness of current multistakeholder processes.
- The establishment of the DCF is based on the notion of tripartite engagement, which can potentially sideline the interests of the technical community and end users through their omission as important stakeholders.
- This new process would effectively be a state-led process that ultimately lacks transparency and prioritizes the interests of states over other stakeholder groups.
- The proliferation of new Internet governance fora is a burden on time and resources for various stakeholder groups.

Suggestions

- Rather than establishing a new Digital Cooperation Forum, we recommend maintaining the IGF as the main UN platform for Internet governance discussions. The IGF could further be developed to include mechanisms for follow-up actions.
- Reaffirm a commitment to multistakeholder processes to deliver an inclusive, open, free, secure, accessible, and interoperable Internet
- Recognize the technical community as an integral part of the multistakeholder model so that its expertise is provided on matters that pertain to the stability and security of the public core of the Internet.
- Given the essential and global nature of the Internet, it is crucial to increase digital literacy and capacity building among all stakeholders (including governments, legislators, businesses, and the general public).
- Promote open data initiatives to enable the sharing and utilization of information for the public good.

Theme 6. Data protection and empowerment

Considerations and comments

We support the Digital Global Compact Brief 5's proposal to **establish common definitions and standards** for data protection, and encourage the adoption of the OECD's privacy principles, which serve as the foundation for the majority of privacy laws globally, reflecting

- Collection Limitation
- Data Quality
- Individual Participation/Consent
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Accountability

We recognize that **privacy** is an inalienable and universal human right, and has been recognized as such under article 12 of the Universal Declaration of Human Rights, and article 17 of the International Covenant on Civil and Political Rights. At the same time, we also recognize the substantial burden placed on individuals within the context of data protection, and the concept of "consent fatigue" (e.g. GDPR 'cookies fatigue') or the "privacy paradox".

We have a strong concern that a shortage of **capacity** in exposed areas might be a blocker for implementing a thorough and informed process for data protection.

Suggestions

With above-mentioned considerations in mind we propose the following actions to be included in the Global Digital Compact (GDC).

- A core principle for the GDC should be the establishment of a "global minimum" baseline for data protection and empowerment, to aid international interoperability, reduce compliance burdens, and "jurisdictional shopping", that can be supported across the diversity of UN members, but that is also *implementable* and *enforceable* even in nations with limited capacity, especially the Global South.
- Consistent with the global nature of the internet, data protection authorities and the Global Privacy Assembly should be consulted by relevant stakeholders in the internet ecosystem, to ensure the right to privacy is upheld.
- We propose that the GDC empower existing multistakeholder bodies like the IGF to support and inform data protection governance efforts, rather than creating new institutions or initiatives.
- We propose a data protection capacity building initiative, including training and funding instruments, to support member nations and civil society actors, particularly in the Global South, to develop capabilities to govern data domestically and engage internationally. For example establishing a new track within the IGF to ensure that they

set up standards and proof compliance. Or creating shared capacity for data-related complaints and investigation, such as Global Data Protection Ombudsperson or Commissioner that could act on behalf of individual nations or groups of nations.

- This compliance exercise could then be multistakeholder, as every actor in a particular country could comment on how the standards are implemented.
- Reflecting that policies to assure "informed consent" by citizens/consumers has proven challenging and at times frustrating to achieve in practice, GDC efforts should focus on principles of *transparency*, *interoperability*, *self-determination* and *economic empowerment*, *necessity*, *proportionality*, *minimal intrusiveness*, and *effectiveness* for all personal data processing.
- We support efforts to empower citizens, civil society groups, academic researchers, businesses and other non-state stakeholders, with the focus on transparency empowerment in use of personal data. One could look to Estonia to evaluate their data transparency application, the [Data Tracker](#), which allows users to see how governments and private actors are using their data.

Theme 7. Agile governance of AI and other emerging technologies

Considerations and comments

We strongly advocate that agile governance of Artificial Intelligence (AI), as well as any emerging technology, should ensure the development, deployment and use of the technology observes human rights, democracy and the rule of law. We endorse a safe use of AI and emerging technologies mitigating its risks by accounting for hard and soft law, existing and future regulations, and national and international guidelines, including regulatory sandbox initiatives.

The governance of AI and other emerging technologies need not be built from the ground up; they fall under existing legal and regulatory frameworks, notably for data protection and privacy but also IP/copyright, competition, communications regulation, and others. The future frameworks can build upon these existing regulations by strengthening and expanding them in order to cover the fast evolving emerging technologies, whilst awaiting the creation of a cross-cutting regulation.

There are already [many principles](#), [best practices](#), national strategies, and other instruments on AI that GDC efforts should bridge from, promoting a safe and collaborative environment for both companies and individuals, always towards the socioeconomic development of all humanity. It is important that a common place to discuss regulations be established - possibly within the already existing forums to avoid fragmentation of efforts.

We applaud the Global Digital Compact Brief 5's proposal to agree with industry associations to develop sector-based guidelines, reflecting that applications of emerging technologies differ across industries (e.g. agriculture, health care).

Suggestions

With above-mentioned considerations in mind we propose the following actions to be included in the Global Digital Compact.

Actions for All Stakeholders:

- The GDC proposal for supporting sector-based guidelines could go further, directly providing support for the convening industry sector-specific initiatives to develop guidance and standards for AI and other emerging tech.
- To avoid duplication of processes and internet fragmentation we suggest strengthening the Policy Network on AI (PNAI) in the IGF rather than creating a new advisory body as suggested in the GDC.
- The proposal for a global collaborative research and development initiative should prioritize the monitoring and publicizing of information about emerging technologies for different sectors (i.e. sharing of findings for the practical purpose of informing governance).

- There needs to be a guarantee of the right to informational self-determination, notably by ensuring that individuals are always informed appropriately when they are interacting directly with an AI system or when they provide personal data to be processed by such systems.
- Promoting capacity building and education on AI and other emerging technologies, especially in the Global South, to enhance human resources to develop tools that consider the specific problems and necessities of AI, from both a legal and a technical perspective.
- We encourage all stakeholders to engage with policy makers and legislators.

Actions for Governments:

- Giving preference to decision-making processes based on multi-stakeholder approaches.
- Take into account that agile governance processes should broadly be technology neutral to take future innovation into account. The idea is not to regulate the technology but its use, the technology in itself should be able to continue and foster innovation.
- Hold organizations responsible for adverse impacts caused by their AI systems, for example by appointing qualified individuals to assess AI conformity with privacy laws, competition laws, communications regulation, and others.

Actions for the Private sector:

- Investing in the explainability of Artificial Intelligence tools, respecting the best techniques available on the market and in constant collaboration with the development of improved techniques by the scientific community, which can be fixed by sector-based guidelines.
- Investing in human review of automated decisions, at least on the topics with a high-risk impact on human rights, according to Ethical Impact Assessment (EIA), such as recommended by UNESCO's Recommendation on the Ethics of Artificial Intelligence.

Fellows participating in preparing the statement

- Alona Borzhemska
- André Côté
- BLakshi Bhatia
- Bukola Faturoti
- Cecilie Thi Lam
- Dal Singh
- Felix Loxen
- Gulalai Khan
- Isabelle Lois
- Jean Ferreira
- João Pedro Martins
- Johannes Hilling
- Karolina Larsson
- Kasian Emmanuel
- Kjerstin Burdick
- Maeva Devoto
- Mari Malvenishvili
- Nataliia Pohorska
- Neema Lugangira
- Rafaela Ferreira Gonçalves da Silva
- Sabrina Heber
- Samuele Fratini
- Sanna Wolk
- Sarah Opendi
- Sophie Mitchell
- Sorene Assefa
- Tomoe Watashiba
- Vivien Schönberger